

**THE INFLUENCE OF SOCIAL MEDIA ON CRIMINAL BEHAVIOUR AMONG
CONVICTED INMATES**
(A STUDY OF NIGERIAN CORRECTIONAL INSTITUTION KIRIKI, APAPA LAGOS
STATE)

OLADIPO EUNICE MOLAYO

Department of Administration and Management
Crawford University, Igbesa, Ogun State, Nigeria

AKINLOTAN, RAYMOND ADENIYI

Department of Social Sciences
Crawford University, Igbesa, Ogun State, Nigeria

AKAZUE GLORIA DEBRAH

Department of Social Sciences
Crawford University, Igbesa, Ogun State, Nigeria
&

OMODAJI, RUKWE BLESSING

Department of Social Sciences
Crawford University, Igbesa, Ogun State, Nigeria

ABSTRACT

This study explores the influence of social media on criminal behavior, highlighting both its facilitative and preventive roles. With the rise in global social media usage, platforms like Facebook, Instagram, Twitter, and TikTok have increasingly become arena where various forms of criminal activities such as cyberbullying, cyber fraud, phishing, and extortion are perpetrated. The study examines how the anonymity, widespread reach, and rapid dissemination of information inherent in these platforms contribute to the proliferation of such crimes. Drawing on theories such as Social Learning Theory and Routine Activity Theory, the research provides a theoretical lens for understanding how social media interactions may normalize or encourage criminal acts. Utilizing a quantitative research design, data was collected via structured questionnaires administered to 100 male inmates incarcerated for cybercrimes at the Kirikiri Maximum and Medium Custodial Centers in Lagos, Nigeria. The findings aim to enhance the understanding of the complex relationship between social media and criminal behavior, offering insights for law enforcement, policy-makers, and social media users to develop effective preventive strategies and promote safer online environments.

Keywords: Social Media, Online Criminal Behaviour, Cybercrime, Phishing.

Introduction

Generally, Social media has undeniably reshaped the outlook of communication and interaction, between various aspects of societies, which also include criminal behavior. With more than 3 billion users worldwide social media platforms like Facebook, Twitter, you-tube, Instagram and Tik-Tok have revolutionized how individuals interact, share information and

others form communities (Simon Kemp, 2023). Social media has become an essential part of human life. Despite the fact that social media brings great convenience to humans, the ubiquity of social media platforms has influenced the way people perceive crime and the levels of criminal behaviours. According to related literature, social media consumption could increase individuals' sense of fear about criminal behavior, and regions that have high levels of social media usage have spatial similarities with regions with high crime rates. Moreover, some studies discovered that the relationship between social media usage and crime rate could be very complicated. The correlation between the two factors could be positive and negative in different regions of the world. With the awareness of social media's profound influence, people would work through concerted efforts in the future in order to maximize social media's full potential while guarding people's safety.

The use of social media platforms helps users to share their daily lives, experience ideas and engage with others on social media. However, this freedom and the anonymity offered by these platforms can also encourage criminal activities. Criminal activities includes Cyberbullying, harassment, fraud, identity theft, and the dissemination of misinformation are just some of the crimes facilitated by social media's virtual networks (John Whittaker and Rebecca Kowalski, 2020). The nature of content on these platforms means that criminal acts can quickly escalate, and can pose a threat to the society (David Wall, 2015).

Social media also contribute to the rise of unlawful act, this includes cyberstalking, and financial frauds. Criminal uses social media to deceive victims, and also impersonate individuals or group of organizations. This anonymity that is being offered by social media can make it easy for criminals to escape police officers and continue with their illegal activities without anyone knowing. Drug trafficking networks now bypass traditional distribution methods and utilize social media to reach potential customers directly (U.S. Department of Justice, 2021). Additionally, human trafficking, where offenders use platforms to lure vulnerable individuals into exploitative situations, has become a pressing concern (Mark Latonero, 2018). Extremist groups also use social media to spread propaganda, recruit new members, and coordinate violent attacks (Maura Conway, Lisa McInerney, and Sarah Jane Nissen, 2019). The viral nature of social media can amplify the impact of criminal events such as mass shootings, riots, or terrorist activities, as these incidents can quickly gain widespread attention and incite further violence or unrest (David Omand, Jamie Bartlett, and Carl Miller, 2012).

The influence of social media on crime would be multifaceted and complex. Just like any other communication tool, it could be used in both positive and negative ways. Social media could bring people together to fight against crime, and police organizations could use social media to gather the information they need. On the other hand, the unregulated nature of social media provides platforms for cybercrime, such as cyberbullying and online harassment. Criminals could also use the help of social media to perpetrate all kinds of digital frauds. The anonymity of social media also puts a barrier for police to locate criminals on the internet. Moreover, the unbelievable speed of information spreading on social media also has great threats. The past has proven that false information and rumors spread like wildfire on social media, which may easily cause public fear and chaos.

As a result of this, the goal of this study examines both the negative and positive influence of social media on criminal behavior.

Statement of the problem

The rise of social media has profoundly transformed how individuals communicate, share information, and engage with the world around them. While these platforms offer numerous benefits for connectivity and information dissemination, they have also become fertile grounds for various forms of criminal activity (Brian Jensen, 2017). Criminals now exploit social media for cyberbullying, fraud, human trafficking, illegal drug sales, and the spread of extremist ideologies (Susan Brenner, 2021). The anonymity, global reach, and vast user base of platforms like Facebook, Twitter, and Instagram allow perpetrators to target victims without geographical limitations, making it difficult for law enforcement to identify, track, and apprehend offenders (Petter Gottschalk, 2019).

The rapid spread of misinformation on social media further complicates this issue, as it can incite violence, promote hate crimes, and even spark civil unrest (Caroline Jack, 2017). Criminals and bad actors exploit the viral nature of social media to amplify their influence, turning these platforms into breeding grounds for criminal activity when not properly regulated or monitored (Alice Marwick and Rebecca Lewis, 2017). Hence, the problem lies in understanding how social media simultaneously facilitates criminal behavior.

Research Objectives: The specific objectives are to:

- i. Examine how social media help in promoting Cyber bullying.
- ii. Investigate how social media aid in Cyber Fraud.
- iii. Examine how social media help in promoting Phishing.
- iv. Investigate how social media aid in Extortion.

Research Questions: This study seeks to address the following critical questions:

- i. How does social media help in promoting Cyber - bullying?
- ii. How does social media promote Cyber Crime?
- iii. How does social media promote Phishing?
- iv. How does social media aid in Extortion?

Significance of the Study

The study is important for several reasons, but most importantly, this research work contributes to the growing body of knowledge on the dual role of social media as both a facilitator of crime and a tool for crime prevention. It will also provide valuable insights for law enforcement agencies on the most effective ways to utilize social media for crime detection and prevention while addressing the challenges of privacy, jurisdiction, and misinformation.

Scope of the study

The study aims to investigate the role of social media in crime prevention and investigation within the male section in the Kirikiri correctional center in Apapa Lagos, Nigeria.

Literature Review

Over the past two decades, social media has revolutionized the way people communicate, interact, and share information. Platforms such as Facebook, Instagram, Twitter, and TikTok have evolved into powerful tools for networking, entertainment, and information dissemination. However, the same platforms that facilitate social connections have also become fertile grounds for criminal activity. As social media use has become ubiquitous, the rise of crime in the digital space has become a growing concern for the society.

Research highlights that social media platforms can serve as a double-edged sword—on one side, they enhance connectivity and information flow, while on the other, they create new opportunities for crime (David S. Wall, 2007). Criminals are increasingly exploiting the wide reach, anonymity, and ease of use of these platforms to commit a range of offenses, from cyberbullying and identity theft to more complex activities such as terrorism and human trafficking (Kyung-shick Choi, 2008). Understanding the relationship between social media and criminal behavior requires delving into the ways in which these platforms shape deviant behavior.

The characteristics of social media make it an attractive tool for criminals. First, the vast amount of personal information users voluntarily disclose provides criminals with data that can be exploited for illegal purposes. Traditional crimes like fraud, harassment, and extortion have migrated online, while new forms of criminal activity, such as phishing scams and ransomware attacks, have emerged. Social media is often a key component in these crimes, either as a tool for criminals to find victims or as a medium for facilitating illegal transactions. Moreover, organized crime syndicates have embraced social media to recruit new members, coordinate criminal activities, and even boast about their illicit exploits.

The anonymity and rapid dissemination of information on social media can also contribute to more serious forms of criminal behaviour, including terrorism and radicalization. Terrorist organizations have increasingly turned to social media as a recruitment and propaganda tool. Platforms like Twitter and Telegram have been used to spread extremist ideologies, recruit vulnerable individuals, and coordinate attacks. The 2015 Paris attacks, for instance, highlighted how terrorist groups like Islamic State Iraq and Syria (ISIS) effectively used social media to plan and execute their operations, often evading detection by law enforcements (Laura Huey, Johnny Nhan, & Ryan Broll, 2013). The decentralized nature of social media makes it particularly difficult for authorities to monitor and regulate these activities, creating significant security challenges. Additionally, human trafficking and exploitation have found a new venue in the digital world. Traffickers use social media to identify, groom, and exploit victims, particularly young and vulnerable individuals. Studies show that traffickers often create fake profiles, posing as potential friends or romantic partners to lure victims into exploitative situations (Mark Latonero, 2011). The ability of traffickers to conceal their identities and operate across borders complicates rescue efforts and prosecutions. In many cases, victims themselves may be unaware that they are being manipulated through social media until it is too late. Furthermore, social media plays a critical role in the spread of misinformation and the perpetuation of criminal behavior. Viral “challenges or trends sometimes promote illegal activities, such as vandalism, reckless behavior, or drug use. The "Blue Whale Challenge" is an infamous example of how social media can be used to

manipulate vulnerable individuals into engaging in dangerous or illegal acts, sometimes leading to self-harm or suicide (Liliana Pereira, Daniel Cardoso, & Rosa Neves, 2019).

Cyberbullying is a very serious issue on social media and has been increasing in prevalence over the past few years. Cyberbullying (cyber harassment or online bullying) is a form of bullying or harassment using electronic means. Since the 2000s, it has become increasingly common, especially among teenagers and adolescents, due to young people's increased use of social media. Related issues include online harassment and trolling. In 2015, according to cyberbullying statistics from the i-Safe Foundation, over half of adolescents and teens had been bullied online, and about the same number had engaged in cyberbullying. Both the bully and the victim are negatively affected, and the intensity, duration, and frequency of bullying are three aspects that increase the negative effects on both of them.

Types of Cyber-bullying

(i) Cyberstalking

Cyberstalking is a form of online harassment in which the perpetrator uses electronic communications to stalk a victim. This is considered more dangerous than other forms of cyberbullying because it generally involves a credible threat to the victim's safety. Cyberstalkers may send repeated messages intended to threaten or harass, and they may encourage others to do the same, either explicitly or by impersonating their victim and asking others to contact them.

This can be a combination of most of the other methods in order to stalk someone using electronic means. This can include finding the victims location, harassing them with spam, or using sextortion. An example of this situation occurring is when Paris Deshaunte Evitt, a 30-year old from Tulsa cyberstalked one of his former partners. A news article on it states, "Between October 2018 and continuing until October 2020, Evitt used email, Facebook, and text messages to control and threaten the victim. However, his abuse of the victim had started years before. Between 2012 and 2019, Evitt was convicted on 5 different occasions for physically abusing the victim including strangulation, assault, and interfering with reporting. Evitt was also on state supervision at the time of the current offenses. (The unidentified victim) explained that Evitt had destroyed her sense of security and became emotional when she discussed Evitt's statement that he would rather see her dead than happy. She also stated, 'the longer he is away from my children and I, the more time we have to try and heal and move on with our lives, if that is even possible.

(ii) Trolling

Internet trolls intentionally try to provoke or offend others in order to elicit a reaction. Trolls and cyberbullies do not always have the same goals: while some trolls engage in cyberbullying, others may be engaged in comparatively harmless mischief. A troll may be disruptive either for their own amusement or because they are genuinely a combative person. Trolling can include insults, false news, or, terrorist threats.

(iii) Hate Raids

On Twitch and other live streaming services, hate raids are situations where a stream is "raided" by many viewers who flood the chat with harassment and other hateful messages.

This prevents the streamer from executing their stream. These viewers are typically automated bots, making it difficult to moderate and block.

(iv) **Spam**

Spamming is the act of creating multiple accounts and sending messages to a target en masse. A common situation where spam can occur is after a breakup. If one partner is obsessive, they may send their ex messages on multiple platforms. This often happens despite being blocked by the recipient. The article What Can Police Do about Harassing Texts? States, "Keep in mind that harassment of any kind is illegal and includes in person, over the phone, via text messages, through social media, or any other method. Some laws are in place about cyber-bullying that are designed to protect the public from this happening.

(v) **Impersonation**

Impersonation is the act of pretending be another person. If the offender pretends to be the victim, they may say or do things to hurt the victim's reputation. This can include hacking into a Twitter account and spreading disinformation. One famous example is when Sony Music's Twitter account was hacked and posted the following statement: "Britney Spears is dead by accident! we will tell you more soon. #RIPBRITNEY. Spears was, in fact, alive and well.

(vi) **Doxxing**

Doxxing is the act of disclosing a victim's personal data, such as their home address, phone number, and full name. Doxxing can happen when fans in fandoms with large fanbases often go too far when protecting their idols and enter the realm of cyberbullying. Extreme fans of the K-pop music genre sometimes dox fans of rival music groups. This specifically was shown in an incident where fans of the group Blackpink doxxed the owner of a Twice fan account, sending him to a hospital. This is allegedly because a Twice member disrespected a Blackpink member.

(vii) **Sexual Harassment**

Online sexual harassment is considered a form of cyberbullying. Sextortion, a form of sexual harassment, is the act of coercing a person into sharing intimate images before threatening to release them unless money is paid. It is a specific type of blackmail. The line between sexual harassment and cyber-bullying is blurred.

The Internet continues to influence and enhance many aspects of daily life. Faster connectivity, increased communication, and access to broader libraries of entertainment are all considered positive contributions to the user experience. However, there is growing recognition that the same technologies can also provide an opportunity to amplify negative behaviour online, with social media often used for engaging in antisocial activities. Consequently, cyberbullying on social media has emerged as a growing widespread problem due to increased likelihood of encountering strangers online with hidden ulterior motives or tormenting behaviors that lead to bullying, harassing, or intimidation against an individual or group. Existing literature has highlighted the psychological and physical impact of this negative behaviour with increased depression, anxiety, substance abuse, self-harm, and suicidal thoughts all shown to occur. Several factors appear to contribute to the prevalence of

cyberbullying on social media, including anonymity, easy access to technology, inadequate awareness of the consequences of online behavior, and the necessity for effective interventions to prevent or mitigate cyberbullying. These contributing factors can manifest in a range of cyberbullying-related behaviors, in particular, flaming, trolling, and harassment, each with its distinct characteristics and impact on the victim. In addition, examined the problem of anonymity on social network sites where perpetrators can masquerade as different fake personas with multiple online accounts to target their victims. Adolescents and young adults have been observed to be the most at-risk groups, with females reporting higher victimization rates than males. Moreover, female victims are more likely to experience social anxiety and sleep problems, while male victims are more likely to engage in antisocial behaviours due to previous negative experiences. Recent studies have also highlighted the prevalence of cyberbullying among adults and its negative impact on mental health. Despite a growing body of knowledge, Cyberbullying limitations exist beyond the use of self-reported data, small sample sizes, and a narrow focus on specific social media platforms. Notably, there appears to be a lack of consistency when defining cyberbullying, leading to an array of confusion in the findings. In addition, there appears to be a lack of consensus regarding the extent and direction of the association between social media use and mental health. Some studies suggest there is a negative relationship between mental health, well-being, and social media, whilst other research reports a lack of association. As such, it is agreed that future research should focus on examining the impact of cyberbullying on social network users and aid in the development of effective cyberbullying prevention and intervention strategies. This systematic review presents a comprehensive synthesis of the current literature on cyberbullying, offering a detailed overview of its definition, reported prevalence, and impact. Crucially, it highlights two significant gaps in the existing research, first, it reveals that cyberbullying amongst adults is an under-researched demographic, suggesting a need for more focused studies in this area. Second, it identifies notable inconsistencies in the definition of cyberbullying across the literature, indicating a pressing need for a unified conceptual framework. This work not only consolidates the diverse strands of research in cyberbullying but also sets the stage for more targeted and cohesive future studies.

The Role of Social Media in facilitating Cybercrime

Social media has been used since last two decades. Social media was used to send mails and even small messages to your loved ones, than it evolved to a much bigger platform so that people can reach out to unknown people from around the world or maybe to people who are like them (sharing same interests). It created a space for everybody to send messages and showcase their memories, photos or sharing their personal details like location, phone numbers etc.

Social media emerged to the ultimate level of socialism, since last 5 years or majorly during Covid people consumed content like never before. They saw news, music, sports, socializing to complete strangers for hours, chat in different rooms and be friends with people even educate themselves or learn from others. According to [BRITANNICA], cybercrime is the use of computers as tools to achieve illegal ends, such as fraud, trafficking in child pornography and intellectual property, identity theft, and invasion of privacy. Cybercrime, especially through the Internet, is becoming increasingly important as computers become central to commerce, entertainment, and government.

One of the first cybercrimes was hacking which dates back around 1960's and 1970's and it was all because of the curiosity and desires of the people to explore the technology. With the advancement of internet cybercrime kept on growing and took more of a serious form. In the late 1970's it all started with phone system hacking but now it has taken all sorts of forms (for an Example - malware to disrupt systems and steal information, phishing scams for money (online fraud), cyber terrorism to attack political and ideological goals. Nature of cybercrime is no different than the nature of actual crime. People get robbed, information leakage, harassment, public humiliation etc. Everything is same it's just the type of form in which it's taking place.

(i) Social Media: The Gate for Cyber-Crime

Social media in as much as has brought about a change in the way people communicate and interrelate has equally become a hunting ground for cyber criminals. The scope, richness of the data that the users provide consciously or unconsciously and interconnectivity of these platforms make them viable targets for malevolent actors. Regarding this topic, this essay will essentially discuss how social media acts as an entry point of cyber-crime, special weaknesses and forms of attack.

(ii) Data Harvesting and Profiling

Data harvesting and profiling are some of the principal methods used by social media in the encouragement of cybercrime. People give out lots of details that can reveal their identity and other issues such as residential details, their age, and even their financial details on these platforms. Such data enables the attacker to build a detailed profile of the intended target, and therefore map out ways to attack the intended target effectively.

(iii) Phishing and Social Engineering

While phishing involves creating fake emails or messages with the intent of duping people into divulging their identity details, social media has made it easier for cyber criminals to perpetrate this cyber-crime. Some potential details that could be obtained from an SMM profile include password information theft, which will give the attacker full control of an individual's account, identity theft, stalking, and hacking of someone's social media account.

(iv) Malware Distribution

Social media also poses another threat in that it provides a platform through which malware can be spread through malicious downloads and links such as viruses, malware, and ransomware. Hacking groups could publish links to malicious websites or email attachments which, if opened or downloaded, would harm the owner's device and steal their information.

(v) Identity Theft

People's detailed personal information is often what thieves aim to steal. Once they get their hands on this data, they don't waste time. They start crafting fake identities and soon they're out there making off with things like credit cards and loans pretending to be someone else.

(vi) Cyberbullying and Harassment

Social media has become a place where cyberbullying and harassment persist. Sites let anyone sign up and stay hidden behind a screen, which means some individuals behave badly

without facing any consequences. Researchers have found that victims of cyberbullying often face tough emotional and psychological effects like feeling really down, worried all the time, and even thinking about suicide.

The advent of technology has made it possible for nations of the world to integrate with one another and to create a bond with other nations to the extent that the entire world has become like a “global village”. This paved the way for the electronic market to be opened to everybody, and this has also created room for all manner of individuals to seek for people who they can do business with notwithstanding the continent where the business partner resides. This has created room for fraudulent individuals to find a fertile ground in order to dupe innocent people who fall prey to scammers on the internet. The primary function of the social media is to provide people with the platform to socialize. Unfortunately, social media have exceeded the primary design, serving a multitude of other roles since its inception. From contest and advertisements to breaking news and awareness creation, the social media platform is the most efficient/effective means to communicate in this digital age (Hughes, 2014). Among the many changes of the modern world, it is the social media that plays a pivotal role.

Durkheim (2013) sees crime as an integral part of a society and a normal society phenomenon in the sense that it existed in all societies throughout history. To Durkheim, stealing via the use of social media network, is a crime which violates social norms, and works against the functions of society as a means of defining the limits of behavior that are acceptable, serving as an instrument for social change by extending and putting to test those boundaries (Abayomi, 2013).

However, information technology revolution associated with the use of social media has brought about two-edged functions: On one hand, it has contributed positive values to the world, while on the other hand, it has produced so many maladies that threaten societal order and also a new wave of crime to the world. The social media, which ordinarily should be a blessing as they expose one to a lot of opportunities in various fields of life are fast becoming a source of discomfort and worry due to the atrocity being perpetrated through them.

Shinder (2002) defines cybercrime as an offense committed by using the internet or another computer network as a component of the crime. Cybercrimes are offences that are committed against individuals or group of individuals with a motive to intentionally, harm the reputation of the other or cause physical harm to the victim directly or indirectly using modern telecommunication networks like the internet or smart phones. Such crimes may threaten a nation’s security and financial health. The causes of cybercrimes are not far-fetched. One only has to take a quick glance around the society to observe illicit wealth acquisition and its display. This is coupled with the fact that the perpetrators are highly exalted. The problem is made worse by the high youth unemployment, negative role models, the absence of enforceable prohibitive laws, and the general laissez-faire attitude of individuals and businesses regarding cyber security (Hassan, Lass & Makinde. 2012).

As risky as it can be to do business via the social media platforms, many corporate organizations, including banks, still depend on ICT and computer networks to perform basic

as well as complex tasks without being afraid of failing into the booby trap of internet fraudsters. The electronic market is however open to everybody, including criminals. There are many effects of cybercrime; Hassan et al. (2012) identify them as reduction in competitive edge of organizations, time wastage and slow financial growth, slow production time and increase in overhead cost, as well as defamation of the image of a nation. Other major effects include monetary losses and loss of privacy. An organization can lose its competitive advantage and suffer losses when a hacker steals its confidential information and plans, and sells it to a competitor. The time spent by IT personnel on rectifying harmful incidents caused by cyber criminals could have been used to earn profit for the organization. The financial costs to economies and businesses from cyber-attacks include the loss of intellectual property, financial fraud, and damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc.) make up a proportion of the reported cost of cyber-attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. Businesses face greater damage from financial fraud and intellectual property theft over the Internet.

One key negative effect of cybercrime is that it tarnishes a country's image. Once a country is labeled as a harbor for cybercrime activities, potential investors are cautious in investing in such countries. This has some dire implications for the nation's macroeconomic stability, it retards financial growth, and proliferation of cybercrime in a particular country can discourage financial inclusion due to the fear of being a victim of cyber-attack.

Social media phishing refers to an attack executed through platforms like Instagram, LinkedIn, Facebook TikTok, or Twitter. The purpose of such an attack is to steal personal data or gain control of your social media account.

Social media has become as ubiquitous as the air we breathe. Individuals use Facebook, Instagram, Twitter, and a multitude of other platforms to keep up with friends and family, stay on top of the latest news, date, and connect with the world.

Businesses also use social media to keep customers informed about their latest product offerings and events, for marketing, and to attract new business. This makes social media an attractive platform for threat actors to execute phishing attacks. Tools such as Hidden Eye or Shell Phish make these types of phishing attacks as easy as running an application. The information gleaned by the hackers includes social media account login credentials, credit card information, and personal information about you that can then be used to launch other scams and attacks.

(a) Instagram phishing

Instagram is a popular photo- and text-sharing platform. Instagrammers worldwide use this platform as sort of a video diary to share everyday activities and moments. A phishing attack on Instagram begins when a hacker creates a fake Instagram login page. To fool you, these sham pages are crafted to look as much like the real site as possible. When you provide an Instagram user ID and password to the phony page, the attacker captures your credentials. You will usually be redirected to the real Instagram login page for authentication, but the damage has already been done. With your Instagram credentials, the attacker has full access to your account.

If you use those same credentials to log on to other social media sites, or worse yet, your bank account, the attacker will have access to those accounts as well. After gaining access to your Instagram account, the hacker can spy on you. The hacker can also now pose as the legitimate user and request personal information from your friends and followers. Naturally, the hacker covers any tracks by deleting fraudulent messages. Taking things to the next level, the attacker can take complete ownership of your Instagram account. The hacker can change your personal information, preferences, and even your password, thus locking you out of your own account.

(b) LinkedIn phishing

LinkedIn is the world's most-used professional networking platform. Hackers send emails, LinkedIn messages, and links to you to con you into divulging sensitive information, credit card data, personal information, and login credentials. The threat actor could hack into your LinkedIn account to pose as you and send phishing messages to your connections to collect personal data. The hacker can also send out emails that appear to be coming directly from LinkedIn. This is possible due to the fact that the official LinkedIn site has several legitimate email domains, including linkedin@e.linkedin.com and linkedin@el.linkedin.com. This makes it difficult to keep up with the authentic domains versus the bogus ones that may be used by an attacker.

(c) Facebook phishing

Launched in the early 2000s, and having over 2.9 billion active users worldwide, Facebook is the king of all modern social media platforms. Sites like Friendster and Myspace preceded it, but Facebook has set the blueprint for how people and businesses connect with friends, family, and customers. A typical Facebook phishing attack is delivered through a message or link that asks you to provide or confirm your personal information. Delivered via a Facebook post or through the Facebook Messenger platform, it is often difficult to separate a prospective friend's legitimate message from a phishing attempt. The information gathered via a Facebook phishing attempt gives attackers the information they need to gain access to your Facebook account. You could receive a message informing you that there is an issue with your Facebook account and that you need to log in to correct the issue. These messages have a convenient link to follow that leads to a Facebook lookalike site. Once you land on this imposter website, you are prompted to log in. From there, the hacker is able to harvest your credentials. Pay careful attention to the URL to be certain you are being redirected to www.facebook.com. Anything else is likely to be a fake.

These phishing attacks can lead to other related attacks, this includes the "pay for followers" attack. In this method of phishing, you receive messages from hackers claiming to provide you with a specific number of "followers" for the low price of five dollars. Providing your personal information and credit card number opens the door for hackers to withdraw funds from your account and/or to log on to your Twitter account and continue the scam across your list of followers.

Phishing scams have been prominent throughout the twenty-first century and continue to evolve, targeting individuals through various means. With the rise of social media as an integral part of society, scammers have increasingly leveraged these platforms to phish individuals worldwide (Fletcher, 2022). While phishing scams are continuously evolving, as

a whole they can be defined by the offender tricking the victim into exposing personal, financial or credential data, mainly via the use of a malicious link impersonating a legitimate website (CISA, 2018: as cited in Alkhali et al., 2021; Williams and Joinson, 2020).

Social media platforms are designed to promote communication through in-app direct messaging between users (Naseer, 2023). While this service allows users to connect with friends online, scammers exploit it to increase the effectiveness of phishing scams. They create fake profiles or hack legitimate accounts to impersonate known individuals or businesses (Maru, 2022). Social engineering is then used to manipulate and persuade users into responding by playing on victims' emotions like stress and empathy (Parsons et al., 2011: as cited in Carroll et al., 2022). This trust is leveraged by scammers to request help from victims, often in the form of money or personal information such as passwords (Terranova Security, 2023). Phishing is particularly effective due to the human tendency to act on trust, which is easily forged online (Tahir, 2021: as cited in Carroll et al., 2022).

As technology advances, phishing scams have adapted to exploit the unique characteristics of social media platforms like Instagram. Unlike email, Instagram encourages users to share personal information through posts, stories, and direct messages, which are visible to both followers and, in some cases, the public, depending on privacy settings (Abbas et al., 2022). Scammers exploit this openly shared information to craft highly personalized spear phishing attacks tailored to Instagram users (Gupta et al., 2016). This adaptation of social engineering techniques, commonly seen in email phishing, thrives on Instagram due to the platform's emphasis on visual content and casual interaction (Parsons et al., 2011, as cited in Carroll et al., 2022). Instagram's design also encourages habitual scrolling and rapid engagement with content, reducing users' attention to detail and making them more susceptible to phishing attempts (Vishwanath, 2015). Phishing attacks pose a serious and rapidly growing threat to users across social media platforms, particularly Instagram (Parker and Flowerday, 2020).

The prevalence of phishing scams on these platforms has surged, with a 103 % increase reported in 2021 (PhishLab, 2022, as cited in Qahri-Saremi and Turel, 2023). This dramatic increase could indicate that social media companies have failed to implement effective protection for their platform users, as the success of phishing attacks is still fuelled by the amount of personal information readily available for manipulation and lack of user awareness to self-protect from phishing attacks (Qahri-Saremi and Turel, 2023). On Instagram, phishing is the most common method scammers use to steal identities and gain control of user accounts (Kaspersky, n.d.). Unlike other platforms, Instagram's focus on visual content and its blend of public and private interactions make it a prime target for scammers, who exploit its interactive nature to deploy phishing attacks like lottery and investment scams (Instagram, n.d.). While Instagram has acknowledged the issue and released educational resources, many users still lack the skills needed to correctly identify and respond to these scams (Bergh, 2018).

Theoretical Framework

(a) Social Learning Theory

Social learning theory is a psychological theory that suggests that people learn new Behaviour, attitudes, and values through observation and imitation of others. This theory has been applied to studying the media and its effects on individuals and society. Albert Bandura's

work on the effect of model observation and the resulting behavior paved the way for social learning theory. Through his work with children, he developed his theory of observational learning. He stated that a person's behaviour is shaped by observing a model and the consequences they face for that behavior. For example, a person may learn not to steal after watching a thief get caught and jailed for his crime.

According to the social learning theory, social media can serve as a powerful influence on an individual's behaviours, attitudes, and values. The social media, including facebook, twitter, instagrm, and other platform on social media, often depict certain behavior's, attitudes, and values as more prevalent or acceptable than they are. This can lead individuals to imitate or adopt these behaviours, attitudes, and values, even if they are not representative of the diversity of human experience. In general, social media can have two sociological effects on its audience. It can normalize certain kinds of behaviours, and it can stigmatize certain kinds of behaviour.

Social media, can play a significant role in normalizing certain behaviours. This is because social media often depicts certain behaviours as being more prevalent or acceptable than they are, which can lead individuals to believe that these behaviours are more common or normal than they are. One example of the normalization of certain kinds of behaviour in social media is the portrayal of violence. Social media often depicts violence in a glamorized or sensationalized way, which can make it seem more acceptable or normal than it is. This can lead individuals to believe that violence is more acceptable or effective in resolving conflicts and may increase aggressive or violent behavior.

Stigmatization occurs when a specific group or idea is negatively labeled or discriminated against by society, and it can have serious consequences for the stigmatized individuals or groups. One way that the media stigmatizes certain things is through the portrayal of negative stereotypes. The media often depicts certain groups or individuals negatively or stereotypically, contributing to negative attitudes and behaviors toward these groups or individuals. For example, the media may portray certain racial or ethnic groups as criminals or lazy, contributing to negative attitudes and behaviors toward these groups.

Social Learning Theory, developed by Albert Bandura (SLT) in 1977 emphasizes how individuals learn behaviour by observing others and the consequences of their actions. This theory suggests that users may mimic the criminal behaviours they observe on social media, leading to an increase in criminal activity across various contexts. For instance, young people may encounter acts of cyberbullying or illegal drug sales which can normalize such behaviours within their own social circles and which can make others feel encouraged to engage in similar actions. Bandura's concept emphasizes that the process of learning is not limited to direct experience but is significantly influenced by the behaviours and consequences observed in others, particularly in environments as immersive as social media. Bandura's seminal "Bobo Doll" also did an experiment in (1961) demonstrating how children are being exposed to aggressive adult models which is more likely to exhibit the same aggressive behaviors , underscoring the study of observational learning. Using social media, users will observe and replicate behaviours, which can include criminal activities, most especially when they see such actions seems normal or being rewarded online.

It is known that people are social creatures. When Albert Bandura first began to champion the notion of imitative responses as a key mechanism in social learning (Grusec,1992), the world was already well aware that people did not learn in a vacuum. The whole of human experience told a different story, one of interaction and cognitive consequence. If anything can be taken from Social Learning Theory, it is this - for better or worse, people observe, imitate, and model the behavior of others ("Social Learning Theory," 2014). It was true in Bandura's day, and it is truer in the age of social media. With this understanding, it is unsurprising that technology eventually provided a platform to digitize the nuances of human experience. Though they are not the first of their kind, Facebook, Twitter, and a variety of other services are now synonymous with daily social interaction, and for the first time in human history, all the world is truly a stage. This new social media paradigm provides a sandbox where imitative behaviors are not only encouraged but are equally rewarded and widely shared.

This emphasize the importance of monitoring online contents to lighten the potential influence of social media on criminal behavior.

(b) Routine Activity Theory

Routine activity theory, developed by Lawrence Cohen and Marcus Felson in 1979, posits that for a crime to occur, three elements must converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian

Motivated offender: Motivated offenders are individuals who are not only capable of committing criminal activity, but are willing to do so. This element that has received the most criticism due to the lack of information regarding what it truly is. A motivated offender can be pointed out as any type of person who has true intent to commit a crime against an individual or property. However, the motivated offender has to be someone who is able to commit the crime, or, in other words, has everything he or she needs to commit a crime, physically, and mentally.

Suitable target: In Routine Activity Theory, the term 'target' is preferred over the term 'victim', as they might not be present at the scene of the crime. For example, an owner of a television might be away from their home when a burglar decides to target the television for stealing. The television is the target and the owner's absence indicates the absence of a capable guardian, thereby making the crime more likely according to the theory. A suitable target is any type of individual or property that the motivated offender can damage or threaten in the easiest way possible. If a target is suitable, this means that there is a greater chance that the crime can be committed, rather than, a target that is hard to achieve. The acronym VIVA provides four different attributes of what makes a target actually suitable, in the judgement of the offender. The acronym goes as follows:

V: Value (The value of achieving the target, in a real or symbolic manner)

I: Inertia (The physical obstacles of the target: weight, height, strength, etc.)

V: Visibility (The attribute of exposure which solidifies the suitability of the target)

A: Access (The placement of the individual, or object that increases, or lessens, the potential risk of the intended attack)

Guardianship: This refers to a person or an object that is effective in deterring criminal offenses, and sometimes crime is stopped by simple presence of guardianship in space and time. A guardian would not necessarily have to be a policeman or a security guard but rather a person whose proximity or presence would lower the chances of a crime happening. This could include a housewife, a doorman, a neighbour or a co-worker. Whilst inadvertent, the presence of a guardian has a powerful impact on the likelihood of a crime taking place. Thus when the guardian is not within the vicinity of the target, the likelihood of a crime occurring is significantly higher.

When applied to the context of social media, routine activity theory helps explain how certain online behaviors and interactions create opportunities for criminal activities. In the realm of social media, individuals engage in routine online activities such as sharing personal information, posting updates, and interacting with others. These routine activities create opportunities for cybercrimes, such as identity theft, online harassment, and phishing scams. The "motivated offender" may be a hacker looking for personal information, a cyberbully picking on a vulnerable target, or a scammer taking advantage of online interactions. People who divulge excessive amounts of personal information or are unaware of the risks associated with using the Internet may be considered a "suitable target." The "absence of a capable guardian" may relate to inadequate cybersecurity precautions or those who are unaware of possible threats.

Social media also create unique environment where motivated offenders can easily identify suitable targets, such as confidential information, while the anonymity of online interactions diminishes the perception of risk associated with criminal actions. This theory provides a strong framework for understanding how social media contributes to various forms of crime by illustrating how everyday activities, coupled with technological advances, facilitate criminal opportunities that might not otherwise exist in offline environments. It is essential to recognize that as individuals increasingly integrate social media into their daily routines, the potential for these convergence points to manifest grows, highlighting the urgent need for enhanced protective measures.

Moreover, during the time of COVID-19 Pandemic altered daily routines, which lead to the increased online activities. This shifted correlated with changes in online fraud. Understanding how change in routine activities can impacts crime issue.

Research Design

Research design refers to the overall strategies or plan that outline how I conducted this study. This study adopted non-experimental research design. The choice of this design is informed by the aim of this study which is to examine the influence of social media on criminal behaviour.

Study Area

Kirikiri Maximum Security Custodial Centre is a prison west of Apapa, Lagos State, Nigeria. It is named after the rural Kirikiri community in which it is situated. A part of the Nigerian Correctional Service, its official capacity is 1,056. It was first established in 1955 during British colonial rule in Nigerian. Paul Chiama of Leadership wrote that "The mention of Kirikiri first

reminds any Nigerian of" this prison. Kirikiri is also an area in Apapa, Lagos. It is also known for housing several important facilities, including prisons, industrial zones, and the Kirikiri Maximum and medium-security sections.

Sampling Technique and Sampling Size

The study adopted the quantitative method of data collection. The respondents were selected through a purposive sampling method under non probability technique. A total of 120 response were incarcerated for cybercrime were selected, 60 questionnaire were distributed to Kirikiri maximum custodian and the remaining 60 were distributed to Kirikiri medium custodian. 60 were retrieved from Kirikiri Custodian and the reaming 40 were retrieved from Kirikiri medium and 20 were misplace.

Primary Source of Data

The primary source of data is original, firsthand information collected directly without any intermediate steps or interpretation. It is data which is obtained mainly from the respondents through the use of questionnaires and interviews to obtain relevant data from the respondents.

Demographic Presentation of Respondents: The respondents were classified into age, gender, Marital Status, Religion, Ethnic Group, Educational Qualification.

Demographic Category	Sub-Category	Frequency	Percentage
Age	15-25	30	29.7%
	25-40	30	39.6%
	40 and above	30	29.7%
Marital Status	Single	60	59.4%
	Married	30	29.7%
	Divorced	10	9.9%
Religion	Christian	50	49.5%
	Muslim	40	39.6%
	Traditional	10	9.9%
Ethnic Group	Yoruba	40	39.6%
	Igbo	40	39.6%
	Others	20	19.8%
Educational Qualification	No formal education	20	19.8%
	Primary education	20%	19.8%
	Secondary education	40%	39.6%
	Tertiary	20%	19.8%

Source: Field Survey, 2025

The respondents were fairly distributed across age groups, with the highest proportion (40%) in the 24-40 age range. This indicates that most participants are in their productive years, which may influence their engagement with technology and criminal behavior. The majority of respondents are single (60%), suggesting that marital commitments may not have been a strong deterrent against criminal activities. Respondents come from various religious backgrounds, with Christians being the majority. This indicates religious diversity among

those involved in cybercrime. The ethnic distribution shows a predominance of Yoruba and Igbo respondents, reflecting the population dynamics of the region studied.

Most respondents had only secondary education, suggesting limited formal education which may relate to their vulnerability to cybercrime participation. A significant 60% of respondents used social media before incarceration, showing its prevalence and potential influence on criminal behavior. Facebook is the most commonly used platform, suggesting it is the main channel through which many respondents engage with others and potentially conduct criminal activities. 70% of respondents witnessed cyberbullying, which reflects the widespread exposure to online harassment. Only 10% reported being victims of cyberbullying. This could suggest underreporting or normal of such behaviors among users. Out of 101 total respondents, 30% admitted to bullying someone on social media. 70% denied involvement in online bullying. 1 person did not answer the question (missing data). This indicates that nearly one-third of the population has engaged in online aggression, showing that cyberbullying is a real and present issue among the sample group. Among those who admitted to bullying, only **10% reported that it caused emotional distress** to the victim. **90% chose "Others"**, which likely includes uncertain, unreported, or unacknowledged effects or unwillingness to admit harm. Again, **1 respondent did not answer** this question. This result may suggest a **lack of awareness or accountability** about the consequences of their actions, or it could point to normalization of online abuse.

The **leading cause** of engagement in cybercrime is **financial need (40%)**, showing that **economic pressure** is a major driving force. **20% each** indicated that **peer influence, unemployment**, and the **normalization of cybercrime in society** influenced them. This shows a combination of **personal financial pressure, peer environment, and social perception**. This suggests that **cybercrime is not only a personal choice but also shaped by social and economic conditions**. It reflects the need for **economic empowerment programs, youth engagement, and public awareness campaigns** to address the normalization of digital crimes in society. Identity theft (50%) and hacking (30%) were the most committed crimes, showing a focus on financial and personal data exploitation. **Half (50%)** of the respondents engaged in cybercrime **3 to 5 times**, and **30%** engaged in it **more than 5 times**. Only **20%** committed cybercrime **once or twice**, which suggests that **cybercrime tends to be habitual or repeated**. The results indicate a **pattern of recidivism**, where once involved, individuals are likely to continue until apprehended. This persistence implies that cybercrime may be **financially rewarding or seen as low risk**, making deterrence through awareness and enforcement crucial. **Phishing** is the leading cybercrime that led to incarceration, accounting for **50%** of cases. This is followed by **cyberstalking (30%)** and **identity theft (20%)**. The dominance of phishing highlights its **effectiveness in deceiving victims** and its **frequency among digital fraud cases**. The results reflect that **phishing is not only common but also highly prosecutable**, likely due to its digital footprint. It also shows where **law enforcement efforts may be most focused**. Facebook is overwhelmingly the platform used for cybercrime, accounting for 80% of the responses, making it a key medium for criminal operations. A large percentage of respondents (70%) reported receiving suspicious messages or links suspected to be phishing attempts. This confirms that phishing is a **common risk on social media**, making users vulnerable to scams. **Facebook** was the most common platform (40%) where phishing messages were received, followed by "Others" (30%). This suggests Facebook is a

hotspot for phishing activity among this group. The unspecified category (.00) may not be clear. **60% of respondents admitted** to phishing before their incarceration. This underlines how common this form of cybercrime is and reflects the **growing trend of financial scams via social media**. A high **success rate of 80%** was recorded by those who engaged in phishing. This demonstrates that phishing not only occurs frequently but also **yields significant results**, making it an attractive crime among perpetrators. A majority (60%) made between **₦100,000 and ₦1,000,000**, highlighting that phishing can be a **lucrative activity**. The earnings indicate strong motivation and possibly a lack of effective deterrence mechanisms. A notable **70% have witnessed extortion via social media**, suggesting that social platforms are being misused not only for fraud but for **coercive or blackmail-like behavior**. **60% of the sample have committed extortion using social media**, showing that this is not just theoretical but **actively practiced** among those surveyed. Half of those involved in extortion **do so frequently**, showing repeated behavior. The **25% who chose "Other"** may include irregular or situational extortion. A large **20.8% did not respond**, possibly to avoid self-incrimination. A striking **87.5% found extortion on social media to be very successful**, indicating its **effectiveness and possibly low risk of detection**. This highlights an area of concern for digital law enforcement. Half of the respondents made **"Other" unspecified amounts**, while **₦40 and above** was also commonly mentioned. This shows **variability in earnings**, but the presence of many "Other" responses may reflect **sensitive or untraceable income sources**.

Presentation of results

Pearson correlation

Social media and cyber bully	Pearson Correlation	1	.095	.409**	.520**
	Sig. (2-tailed)		.347	.000	.000
	N	100	100	100	80
Involvement in cyber crime	Pearson Correlation	.095	1	-.474**	-.595**
	Sig. (2-tailed)	.347		.000	.000
	N	100	100	100	80
Involvement in phishing	Pearson Correlation	.409**	-.474**	1	.640**
	Sig. (2-tailed)	.000	.000		.000
	N	100	100	100	80
Involvement in extortion	Pearson Correlation	.520**	-.595**	.640**	1

	Sig. (2-tailed)	.000	.000	.000	
	N	80	80	80	80
Correlation is significant at the 0.01 level (2-tailed).					

Source: Field Survey, 2025

The correlation table presents the Pearson correlation coefficients that help us understand the relationships between different variables: social media use, cyberbullying, involvement in cybercrime, phishing, and extortion. These correlations reflect how closely related the variables are to one another, and whether these relationships are positive, negative, or neutral. Social media use is moderately positively correlated with cyberbullying ($r = 0.409$, $p < 0.01$), meaning that as individuals spend more time on social media, they are more likely to engage in cyberbullying behavior. This suggests that social media platforms offer opportunities for cyberbullying that may not be as prevalent in face-to-face interactions. Social media also has a strong positive correlation with extortion ($r = 0.520$, $p < 0.01$), meaning that individuals who are more active on social media are more likely to be involved in extortion. The increased presence of personal information on social media platforms makes them ideal venues for extortionists to exploit, using threats or manipulation for financial or personal gain.

In contrast, there is a moderate negative correlation between involvement in general cybercrime and phishing ($r = -0.474$, $p < 0.01$), indicating that those engaged in broad cybercrime activities are less likely to specialize in phishing. This could suggest that people involved in a range of cybercrimes prefer different methods for committing fraud rather than focusing on phishing. A similar strong negative correlation exists between general cybercrime and extortion ($r = -0.595$, $p < 0.01$), suggesting that individuals involved in one of these activities are less likely to engage in the other. This could be due to specialization, with cybercriminals tending to focus on specific types of crime, such as hacking or fraud, without overlapping into extortion.

On the other hand, phishing and extortion have a very strong positive correlation ($r = 0.640$, $p < 0.01$), meaning that individuals who engage in phishing are also highly likely to be involved in extortion. Both activities share a common goal of fraudulent financial gain, and the skills used in phishing, such as manipulating victims into revealing sensitive information, overlap with those used in extortion.

Overall, the use of social media has a statistically significant influence on cyberbullying, phishing, and extortion. The analysis also highlights a strong relationship between phishing and extortion, suggesting that individuals involved in one are likely to engage in the other. Additionally, the relationships between cybercrime and other forms of cybercrime show a tendency for specialization, with individuals tending to focus on one type of crime rather than participating in multiple forms of cybercriminal activity.

Discussion of Findings

The findings of this study shed light on the significant relationship between social media usage and criminal behaviors such as cyberbullying and extortion, as well as the broader implications for understanding the role of social media in modern criminal activities. The

following discussion highlights the key findings and provides a deeper insight into how these results align with existing research and theoretical frameworks.

Social Media Usage and Cyberbullying: The study found a moderate positive correlation of 0.409 between social media usage and cyberbullying, which was statistically significant at the 0.01 level. This suggests that increased social media usage is associated with a higher likelihood of engaging in cyberbullying. The rejection of the null hypothesis in this case indicates a clear relationship between the two variables. The findings align with existing literature, which suggests that social media platforms provide a space for individuals to engage in harmful behaviors like cyberbullying due to the relative anonymity they offer. Social media's potential to amplify negative behaviors, particularly among younger users, is well-documented in prior studies. The ability to post harmful content, harass others, and share defamatory messages or images without immediate real-world consequences makes social media a fertile ground for cyberbullying.

Social Media Usage and Extortion: The study also revealed a strong positive correlation of 0.520 between social media usage and extortion, which was statistically significant at the 0.01 level. This finding suggests that individuals who are more active on social media are also more likely to engage in extortion activities. The rejection of the null hypothesis in this case further supports the idea that social media platforms are often used as tools for coercion and extortion. In the digital age, perpetrators of extortion can exploit personal information, use threats, and blackmail individuals by leveraging social media platforms to manipulate and exploit vulnerable users. This aligns with previous research that highlights how cybercriminals use social media as a medium for extortion, capitalizing on the ease with which personal information can be gathered and shared online.

The Interplay between Social Media and Criminal Behavior: The significant correlations between social media usage, cyberbullying, and extortion underscore a growing concern about the intersection of digital platforms and criminal behavior. Social media is not only a space for positive interaction and communication but also a breeding ground for harmful activities. The study suggests that social media usage is a strong predictor of certain criminal behaviors, particularly among those who have the knowledge and intention to exploit the platforms for malicious purposes.

The results also suggest that individuals who engage in one form of online criminal activity, such as cyberbullying or extortion, may be more likely to participate in other forms of digital crime. The shared anonymity and ease of access to personal information make social media a versatile tool for various types of online crimes. This aligns with the theory of specialization in criminal behavior, where individuals who engage in one type of crime may develop the skills and inclination to engage in other forms of digital misconduct.

Implications for Policy and Practice: The findings of this study have important implications for both policymakers and social media platforms. Given the significant relationship between social media usage and criminal behavior, there is a need for stronger regulations and monitoring of social media platforms. Governments and law enforcement agencies must implement stricter laws to address cyberbullying and extortion, ensuring that those who

engage in such activities are held accountable. Additionally, social media companies themselves must take more responsibility for curbing harmful behaviors on their platforms by strengthening their policies on cyberbullying, extortion, and other forms of abuse.

Educational programs aimed at raising awareness about the risks of social media use and promoting digital literacy can help mitigate the harmful effects of social media on vulnerable individuals. Teaching users about safe online practices, the consequences of engaging in criminal activities, and how to protect themselves from extortion and cyberbullying can reduce the prevalence of these behaviors.

Limitations and Future Research: While the findings of this study provide valuable insights into the relationship between social media usage and criminal behavior, there are some limitations to consider. The sample size, though sufficient, is limited to individuals incarcerated for cybercrime, which may not represent the general population. Future studies could expand the sample size to include individuals outside of correctional facilities to provide a more comprehensive understanding of how social media impacts a broader range of individuals.

Moreover, the study focused on a narrow set of behaviors (cyberbullying and extortion). Future research could explore other forms of cybercrime, such as hacking, identity theft, or online fraud, to provide a more holistic view of the relationship between social media usage and digital criminal behavior.

In conclusion, the findings of this study provide compelling evidence of the significant relationship between social media usage and criminal behaviors like cyberbullying and extortion. As digital platforms continue to evolve, understanding the role of social media in fostering criminal behavior is critical. The results emphasize the need for stronger regulatory frameworks, improved awareness campaigns, and responsible social media practices to mitigate the potential negative impact of social media on society.

. The following major findings emerged from the data analysis:

1. **Social Media and Cyberbullying:** The correlation between social media usage and cyberbullying was found to be moderate and positive ($r = 0.409$, $p < 0.01$). This suggests that higher levels of social media activity are associated with a greater likelihood of engaging in cyberbullying behaviours. The result supports the hypothesis that increased use of social media platforms can expose users to online bullying, either as perpetrators or victims.
2. **Social Media and Extortion:** The correlation between social media usage and involvement in extortion was also found to be strong and positive ($r = 0.520$, $p < 0.01$). This indicates that individuals who use social media more frequently are more likely to engage in extortion activities. The anonymity and widespread access to personal information on social media make it a fertile ground for extortion schemes, which often rely on threats of harm or exposure.

3. **Statistical Significance:** The Pearson correlation results were statistically significant at the 0.01 level for both relationships, confirming that there is a robust connection between social media usage and these forms of criminal behaviour. Thus, the null hypotheses for both cyberbullying and extortion were rejected, supporting the assertion that social media usage does have a significant influence on these criminal activities.

Conclusion

The findings of this study provide clear evidence that social media usage plays a significant role in influencing criminal behaviour particularly cyberbullying and extortion. Social media platforms provide anonymity and ease of access to personal information, which can be exploited for criminal activities.

It is evident from the study that social media is not only a platform for positive interactions but also an environment where harmful activities like cyberbullying and extortion can thrive. The fact that a moderate to strong correlation exists between social media usage and criminal behaviors such as cyberbullying and extortion highlights the need for proactive measures to address the risks associated with online behavior.

The results also show that while social media can foster community building and personal expression, it can also expose users to negative influences. Particularly, the younger population, who are more active on social media, may be more vulnerable to engaging in or falling victim to such behavior.

Recommendations

Based on the findings of the study, the following recommendations are proposed:

(i) Policy and Regulatory Measures:

- (a) **Enhanced Legislation:** Governments should implement stricter laws and regulations targeting cyberbullying and extortion on social media platforms. These laws should hold both perpetrators and social media platforms accountable for allowing such behaviour to proliferate (Hinduja & Patchin, 2018).
- (b) **Collaboration between Social Media Platforms and Authorities:** Social media companies should work closely with law enforcement agencies to detect and prevent cybercrime activities, such as extortion and phishing, ensuring that users are protected from online exploitation (Livingstone et al., 2011).
- (c) **Educational and Awareness Programs:** Cybersecurity Education for Users: Governments, schools, and NGOs should prioritize education on the risks associated with social media. Public awareness campaigns should inform users about the dangers of cyberbullying, extortion, and other forms of digital crime (Vranica, 2019).
- (d) **Parental Involvement:** Parents should be encouraged to actively monitor and guide their children's social media usage. Awareness programs for parents could help them understand how to protect their children from online abuse and prevent them from becoming involved in criminal behaviour (Wright, 2017).
- (e) **Anti-Cyberbullying Measures:** Social media platforms must improve their anti-bullying policies and provide better tools for users to report and deal with

cyberbullying. There should be clear consequences for offenders, and swift action should be taken to remove harmful content (Slonje & Smith, 2017).

- (f) Prevention of Extortion and Phishing: Social media platforms should enhance their security protocols to prevent phishing and extortion attempts. They could implement stronger identity verification methods and improve the monitoring of suspicious activities, thereby protecting users from fraud (Sullivan & Ahn, 2020).

This study has highlighted the significant influence that social media usage has on criminal behaviour particularly cyberbullying and extortion. The findings underscore the need for stronger regulation, greater public awareness, and enhanced security measures on social media platforms. While social media can provide valuable opportunities for socialization and communication, it also presents risks for exploitation and abuse. As social media continues to evolve, it is essential to develop strategies to mitigate its potential for harm, ensuring that it remains a safe and positive environment for all users.

References

- Abayomi, O. A. (2013). The impact of cybercrime on the socio-economic development of nations. *International Journal of Social Sciences*, 25(2), 114-128.
- Akinpelu, O. A., & Sadri, M. (2017). Map of Lagos State showing Apapa, the study area. Kirikiri Maximum Security Prison. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Kirikiri_Maximum_Security_Prison
- Alkhali, M. I., Chiew, L. H., & Williams, J. (2021). Phishing attacks on social media platforms: An evolving threat. *Journal of Information Security*, 29(4), 305-317.
- Bandura, A. (1961). Transmission of aggression through imitation of aggressive models. *Journal of Abnormal and Social Psychology*, 63(3), 575-582. <https://doi.org/10.1037/h0045925>
- Bandura, A. (1977). *Social learning theory*. Prentice-Hall.
- Barker, L. (2019). Social media phishing scams: A rise in malicious links. *Journal of Cyber Security*, 14(3), 45-56.
- Bergh, P. (2018). Educating users on phishing scams: A case study of Instagram's efforts. *Cybersecurity Education Review*, 9(1), 23-34.
- Brenner, S. (2021). Cybercrime and the role of social media. *Journal of Internet Law*, 25(2), 6-12.
- Carroll, J., Parsons, A., & Vishwanath, A. (2022). The psychology behind phishing: Exploiting human trust on social media
- Chiama, Paul. "Nigeria's Famous Prisons " (Archive). *Leadership*. August 7, 2015. Retrieved on March 22, 2016.
- Choi, K.-S. (2008). Social media and crime: The new generation of criminals. *Journal of Cybersecurity*, 6(2), 41-49. <https://doi.org/10.1109/CCS.2008.4737095>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological*
- Conway, M., McNerney, L., & Nissen, S. J. (2019). Extremist propaganda on social media: The role of platforms in the spread of violent ideologies. *Terrorism and Political Violence*, 31(5), 895-916. <https://doi.org/10.1080/09546553.2019.1570457>
- "Even hungry dogs'll reject our meals — Prison inmates". *Vanguard News*. 20 May 2022. Retrieved 22 May 2022.

- Felson, M., & Cohen, L. E. (2010). Routine activity theory and the crime drop in America. *Crime and Justice*, 39(1), 43-97. <https://doi.org/10.1086/652235>
- Fletcher, R. (2022). Phishing in the digital age: How social media platforms are targeted. *Internet Security Journal*, 11(3), 204-221.
- Gabriel, J. A. (2015). Social media and the new wave of cybercrime. *Journal of Digital Crime and Cybersecurity*, 5(2), 52-60.
- Gottschalk, P. (2019). *Cybercrime and law enforcement*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-14323-9>
- Grusec, J. E. (1992). Social learning theory and developmental psychology: The legacies of Robert Sears and Albert Bandura. *Developmental Psychology*, 28(5), 776-786. <https://doi.org/10.1037/0012-1649.28.5.776>
- Gupta, S., Abbas, K., & Vishwanath, A. (2016). Spear phishing on Instagram: Exploiting the power of social engineering. *International Journal of Cyber Security*, 16(2), 114-125.
- Hassan, L., Lass, S., & Makinde, A. (2012). The causes and effects of cybercrime on national security. *International Journal of Information Technology*, 18(6), 78-92.
- Hinduja, S., & Patchin, J. W. (2018). Cyberbullying: An update and synthesis of the research. In J. W. Patchin & S. Hinduja (Eds.), *Cyberbullying prevention and response: Expert perspectives* (pp. 3-19). Routledge.
- Holt, T. J., & Bossler, A. M. (2015). Cybercrime and society: The changing nature of cybercrime in the digital age. *Criminal Justice Review*, 40(4), 403-424. <https://doi.org/10.1177/0734016815580049>
- Huey, L., Nhan, J., & Broll, R. (2013). The Internet, terrorism, and social media: The influence of new technologies on security.
- Hughes, R. (2014). The evolution of social media: From communication to commerce. *Journal of Media Studies*, 10(4), 234-248.
- Instagram. (n.d.). Phishing attacks on Instagram: How to protect your account. Retrieved from <https://www.instagram.com>
- Jack, C. (2017). Misinformation and the role of social media in crime prevention. *Journal of Social Media Studies*, 8(1), 45-63. <https://doi.org/10.1080/2151997X.2017.1309154>
- Jensen, B. (2017). The impact of social media on criminal behavior. *Criminal Justice Review*, 42(3), 270-288. <https://doi.org/10.1177/0734016817733471>
- Jibrin, Adam Abubakar (2018-11-07). "A Visit to Prison Formations in Kirikiri, Lagos". *PRNigeria News*. Retrieved 2021-06-26.
- Journal of Terrorism and Cybercrime*, 9(1), 12-34. <https://doi.org/10.1080/1465005X.2013.781374>
- Kaspersky. (n.d.). How to avoid phishing on Instagram: A comprehensive guide. Retrieved from <https://www.kaspersky.com>
- Kemp, S. (2023). *Digital 2023: Global overview report*. We Are Social & Hootsuite. Whittaker, J., & Kowalski, R. (2020). Cyberbullying, harassment, and social media platforms. *Journal of Criminal Justice*, 48(2), 221-234. <https://doi.org/10.1016/j.jcrimjus.2020.01.003>
- Koski, J. (2021). Phishing and the fast-paced social media environment: A psychological perspective. *Journal of Digital Security*, 7(3), 88-102.
- Latonero, M. (2011). The rise of human trafficking and exploitation in the digital age. *Journal of Human Rights and Technology*, 2(1), 56-69. <https://doi.org/10.1080/17539153.2011.574229>

- Latonero, M. (2018). Human trafficking online: The role of social media in the human trafficking industry. Data & Society Research Institute. https://datasociety.net/pubs/ia_datasociety_2018_human_trafficking_online.pdf
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. EU Kids Online.
- Maru, K. (2022). Social engineering on social media: Impacts of scams and phishing. *Journal of Cyber Security and Behavior*, 23(1), 44-59.
- Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation in social media platforms. Data & Society Research Institute. https://datasociety.net/pubs/ia_datasociety_2017_media_manipulation.pdf
- Naseer, M. (2023). The risks of direct messaging on social media platforms: A threat analysis. *International Journal of Cybersecurity*, 12(4), 56-72.
- "Nigeria: Information on Kirikiri Maximum Security Prison, the type of prisoners kept there, on the structure of the prison, and on the treatment of prisoners." refworld, UNHCR. Retrieved on March 23, 2016.
- "Nigerian prison cells where inmates live like kings, use co-prisoners as servants". Punch Newspapers. 2018-03-03. Retrieved 2021-06-26.
- "NIGERIAN PRISONS SERVICE PRISONS AND CAPACITIES Archived 2016-04-03 at the Wayback Machine." Nigerian Prisons Service. Retrieved on March 22, 2016.
- Omand, D., Bartlett, J., & Miller, C. (2012). The role of social media in crisis communication and crime. *Journal of Law & Cybercrime*, 15(1), 111-126.
- Parker, R., & Flowerday, S. (2020). The rise of phishing attacks in the age of social media. *Journal of Digital Threats*, 22(1), 33-48.
- Parsons, A., Carroll, J., & Vishwanath, A. (2011). The power of social media in phishing attacks: A social engineering perspective. *Cybersecurity in Practice*, 18(2), 77-89.
- Pereira, L., Cardoso, D., & Neves, R. (2019). The Blue Whale Challenge and the dangers of viral trends. *Journal of CyberPsychology*, 13(2), 119-132. <https://doi.org/10.1002/cyber.128>
- PhishLab. (2022). 2021 Phishing trends: A review of attacks on social media platforms. *Cybersecurity Report*, 6(4), 200-210.
- Platforms. *Cybersecurity Review*, 18(5), 99-112.
- Review, 44(4), 588-608. <https://doi.org/10.2307/2094589>
- Shinder, D. (2002). Cybercrime: Understanding the digital threat landscape. *Journal of Information Security*, 10(3), 57-69.
- Shirbon, Estelle; Akwagyiram, Alexis (March 8, 2018). Evans, Catherine (ed.). "UK to build prison wing in Lagos to transfer Nigerian prisoners". Reuters.
- Slonje, R., & Smith, P. K. (2017). Cyberbullying: A review of the literature. In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research* (pp. 34-48). Routledge.
- "Social Learning Theory." (2014). *Encyclopedia of Psychology*, 4th Edition. Oxford University Press.
- Sullivan, M., & Ahn, J. (2020). Phishing and social media: Emerging threats and countermeasures. *Cybersecurity Journal*, 31(2), 124-135.
- Tahir, H. (2021). Psychological manipulation in phishing scams: The role of trust. *Journal of Cybersecurity Psychology*, 8(3), 102-115.
- Terranova Security. (2023). The rise of social media scams: How to protect yourself from phishing. Retrieved from <https://www.terranoasecurity.com>

- U.S. Department of Justice. (2021). Drug trafficking and the internet: Social media's role in the crime network. U.S. Department of Justice.
- Vishwanath, A. (2015). Phishing on social media: The role of rapid engagement in vulnerability. *International Journal of Social Media*, 14(2), 79-94.
- Vranica, S. (2019). Social media education for young people. *Journal of Social Media Studies*, 25(3), 200-214.
- Wall, D. (2015). Cybercrime: The transformation of crime in the information age. *Policing and Society*, 24(4), 363-380. <https://doi.org/10.1080/10439463.2013.869352>
- Wall, D. (2015). The internet as a tool for criminal behaviour . *Criminology and Public Policy*, 14(4), 867-887. <https://doi.org/10.1111/1745-9133.12124>
- Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. *Policing and Society*, 17(4), 413-431. <https://doi.org/10.1080/10439460701412557>
- Whitehead, Eleanor. "Nigeria's addiction to the death sentence." *Al Jazeera*. August 11, 2015. Retrieved on March 22, 2016.
- Williams, J., & Joinson, A. (2020). Understanding phishing: The role of social media in the evolution of cybercrime. *Journal of Cybercrime Studies*, 3(4), 210-225.
- Wright, M. F. (2017). Cyberbullying and its relationship with adolescents' mental health: A review of the literature. *Journal of Youth and Adolescence*, 46(1), 65-75.
- Zahedi, M., & Shloman, S. (2015). Phishing scams in the fast-paced digital world: A study on urgency and compliance. *Journal of Information Systems*, 19(2), 145-160.