Covenant Journal of Informatics & Communication Technology. Vol. 11, No. 2, Dec 2023
ISSN: ***print*** **2354 – 3566** ***electronics*** **2354 – 3507 DOI:**

An Open Access Journal Available Online

Combating Cybercrime Perpetrated Via Social Media Channels Using Individual Resilience Techniques

Francis Alexander Aleke Onyibe[1,*], Glory Nosawaru Edegbe[1], Samuel Omaji[1], Akinola Samuel Olayinka[2]

[1]Department of Computer Science, Edo State University Uzairue, Edo State, Nigeria
[2]Department of Physics, Edo State University Uzairue, Edo State, Nigeria
[*]afraexkonsult@gmail.com/ aleke21.francis@edouniversity.edu.ng; +2348062062303

Received: 18.08.2023, Accepted: 01.12.2023, Publication: December 2023

Abstract—Cybercrime is a social vice associated with modern society due to the rapid development of technology. Various studies over the years have shown that there is no society without an element of cybercrime. Cybercrime also has negative economic implications for nations and businesses globally. Over the years, several approaches have been employed to reduce the rate of cybercrime by employing various combating techniques. Hence, this study explores individual resilience techniques used in combating cybercrime perpetrated via social media channels in Abuja. Three goals and research agendas were developed to guide the research toward achieving the stated goal: a review of relevant literature, a qualitative and quantitative survey design involving about seven million, one hundred and ten thousand internet subscribers that use social media in Abuja, and a sample size of four hundred respondents from the study area were selected using the Taro Yamane purposive sampling technique. The respondents' data were collected using a twelve-item structured questionnaire. Completed instruments of the sample size were analysed using mean values and standard deviations designed using Google Forms. The results showed that identity theft, cyberstalking, malware attacks, and cyber-casing are major cybercrimes perpetrated online by cyber attackers, and these attacks have led to harassment, child exploitation, digital piracy, and intentional damage to individuals' online reputations. However, anti-malware, outlier detection, password managers, and multi-factor authentication (MFA) are various individual resilience techniques social media users can employ to combat cybercrime on social media. Creating more awareness of cybercrime and the various individual resilience techniques required in protecting social media accounts on web-enabled devices and setting up a special task force void of bias to help cybercrime victims regain their assets were recommended.

Keywords/Index Terms—*Social media, Cybercrime, Identity theft, Malware, Cyberstalking, Cyber-casing, and Resilience Techniques.*

1. Introduction

Social media has affected people both positively and negatively in terms of culture, economic, and social life and as well has become an essential part of our daily life (Nwankwo and Ukhurebor, 2020; Asanga et al., 2023). A social media network is a system that permits social media enthusiasts to communicate with one another using multimedia content such as video, text, audio, images, animation, and graphics, and through mediums like websites and apps (Odinakachi et al., 2023; Olusegun et al., 2023; Emeka et al., 2023). This content is cloud-based big data content that can be viewed for quantity, variety, speed, accuracy, volatility, quality, discoverability, and dogma. According to (Abroshan et al., 2021), the growth of digitalization has rapidly increased in the cyber-domain; conceptualization into our daily activities has become an integral of life. People use the internet to do several virtual activities such as business, online studies, knowledge sharing, electronic banking, cryptocurrency, forex trading, and other numerous activities in the real world. However, as cyberspace accelerates innovatively, exploitation exists for personal gain. (Murtaza et al., 2017), despite the continuous improvement of cybersecurity measures, cyberattacks have become a menace in our society. Attackers still exploit vulnerabilities in application designs, web designs, scamming, social engineering as well as other advanced technical methods.

Scamming has been noted to have existed before the existence of computers and the internet (Siddiqi et al., 2022). In cybersecurity, Social Engineering (SE) attacks are perpetrated via scamming or phishing, vishing, smishing, man-in-the-middle (MiTM) attacks, etc. Social engineering deals with the psychological manipulation of individuals to divulge sensitive information (Sharma & Bashir, 2020). According to (Soomro & Hussain, 2019), in March 2019, statistics has shown that the population of Internet users reached 4,168,461,500, equivalent to 50.08% of the world population. According to (Statista, 2020), stated that from 2010–2016, the population of social media users globally was estimated to increase until 2020. In 2018, the statistics were 2.67 billion social media users globally, rising from 1.91 billion in 2014. The rapid use of social media platforms is fast dominating traditional means of communication. Statistically, about 2.31 billion people globally have been noted to be social media users, with a penetration testing of about 31% (Althukair et al., 2021). These users are of different age groups, different cultures, different religions, and different social attitudes and behaviours, and use different devices to connect to social networking sites. The popularity of these websites attracts all kinds of users to these social networking platforms to connect with friends and family, share their social life daily with loved ones and get to know new people which may result in computer crime and internet crime. These social networking platforms attract users from all sectors, collecting their data and storing it in the cloud (Awari & Warjurkar, 2022).

Our lives in today's online world are changing the way we approach privacy and security. A major challenge today is the increase in the volume, speed, variety, and accuracy of data on social networks, which raises several concerns, including privacy and security. However, this major challenge has also proven to be a crime prevention and investigation tool when used intelligently and cautiously. The era is the information age, where there is information everywhere. Today, there are many ways to communicate, such as Twitter, Facebook, other social media tools, blogs, content sharing., communication, and information sharing via photos, videos, mobile messages, etc.

According to Chawki (2005), the computer sneaker "Love Bug" rapidly infected computers worldwide, causing 7-10 billion United State dollars in damage in 2000. In 2004, a 35-year-old British musician murdered his 31-year-old teacher, who was haunted by sexual images he had seen hours before he commit the murder (Argus, 2004). In 2011, metropolitan unrest escalated in many urban areas in the United Kingdom (UK). New social media is said to have been used by participants to disseminate real-time information about incidents and as social coordination to facilitate riots; an example of crime. Fast Internet connections create opportunities for criminals to exploit security flaws in systems. Both cybercrime and traditional crimes are observed on the Internet. This mainly leads to a “haven” for criminals, the new forms of crime discovered by criminals via the use of electronic communication are becoming less publicly recognized (Hinduja & Schafer, 2009).

These attacks occur with the motive of exploiting vulnerabilities caused by human errors. The vulnerabilities exploited as human errors occur because of influence, manipulation, deception, or even persuasion during social engineering (Albladi & Weir, 2020). Most cyberattacks occurring globally are perpetrated without the knowledge of the victims; hence, many internet users have fallen to cybercriminals’ antics, an example is a case of extortionists demanding 50 million United State dollars from an oil giant in Saudi Arabia to be payable in Monero Cryptocurrency (Scott, 2021). Data breach affected over 5 million Marriott customers; the motive of the attackers for exploiting vulnerabilities was to illegally access devices remotely or physically, surreptitiously obtain sensitive information, and breach the cybersecurity measures. Cybersecurity experts on the other hand have continued to develop a methodology or means to thwart the efforts of the cyberattacks perpetrated using social engineering (Josh, 2020).

Social media has now become a public means of communication. Social big data such as tweets, blogs, Short Message Service (SMS), and phone calls can be integrated for crime prevention both in real-time and offline and as well for criminal investigation. Social media is not only a means of passing and receiving information for communities but also a medium for criminal communities. Today, social media is also a tool used by law enforcement agencies to prevent crime (Singh, 2018). However, in real-time monitoring of data, and cloud recognition; Criminal Justice System has been facing challenges related to text, image, audio, and video monitoring. This inability to grip these challenges is attributed to the under-reporting of cybercrime perpetrated on social media channels to the authorities concerned for proper checkmating. This has become a big subject; hampering cybercriminal justice most time (Wall, 2008).

The pacifistic community and the peaceful world are the delusion of all countries, everyone, and all researchers, but there is a possibility of a crime if there is a community. The form of crime has changed from the conventional to the electronic type. The use of social media has increased tremendously; crimes through electronic media are increasing. Criminals employ the use of this real-time on social media to strategize and execute crimes. The law enforcement agency uses a pre-emptive method to control, prevent, protect, and investigate crimes. Also, Individual technology can control crime. Therefore, this review aims to use individual resilience techniques to combat cybercrimes perpetrated through social media channels.

Rapid technological development has skyrocketed the use of computer systems and their networks by individuals, institutions, and corporate organizations in all fields of life globally. Since social media is part of our lives, it is an indispensable tool for humans, and its usefulness and effectiveness have been proven many times, and its use will continue to increase. As part of our lives, the trend of social media platforms has not only contributed to a better life but has also increased the crime rate in our society. The rapid increase in crime on social media has raised many issues, including questions about its effectiveness, but does not affect its social usefulness (Kawasaki & Fitzpatrick, 2013). In a country where the use of social media platform is peaked and online crime has gained the same position as real crime (AbdulRaheem et al., 2022; Adesola et al., 2022a-b), the use of social media by law enforcement agencies and various analysts has become valuable in the prevention, deterrence, and fighting off online crimes (Golbeck & Klavans, 2015; Isah et al., 2016; Omoregbe et al., 2019; Adesola et al., 2019). Thus, this study focuses on using individual resilience techniques to combat cybercrimes perpetrated through social media channels.

Consequently, this study is aimed at examining the individual resilience techniques used in combating cybercrime perpetrated via social media channels. Consequently, attempt will be made to; evaluate various cybercrimes perpetrated by cyber attackers on social media channels using mean and standard deviation; determine the impacts of cybercrimes on social media users in terms of identity theft, cyberstalking, malware, digital piracy, child exploitation, and intentional damage; and ascertain the various individual resilience techniques used by social media users to combat cybercrimes using multi-factor authenticity, anti-malware, and outlier detection, using the following research questions:

1. What are the various cybercrimes perpetrated by cyber attackers on social media users?
2. What are the impacts of cybercrimes on social media users?
3. What are the various individual resilience techniques used by social media users to combat cybercrimes?

In the course of this study, the methodologies and findings will pose great importance to academic students, social readers, and scholars in varied ways. Firstly, this study will depict and bring into the limelight of creating better awareness of the types, and processes of cybercrimes perpetrated through social media channels. Cybercrime on social media channels comes in different forms, it is carried out either by an individual, organization, or a group of well-organized literate individuals who use it as a means of survival. Secondly, through the study, the various impacts of cybercrime on social media users and the individual resilience techniques required to combat cybercrimes will be revealed. This will give reasons to state various coping techniques to avert and control it in the event of occurrence with the sole aim of saving life and sanity. Lastly, this study will also enrich the academic library on issues concerning cybercrimes perpetrated via social media channels adding to the existing literature on the subject matter.

2. Literature Review

2.1. Concept of Social Media

The social media concept varies depending on the school of thought, and the context of use. What an individual understands as social media might differ from what others understand (Granados, 2016) and this was further emphasized by Iñiguez Jiménez et al. (2021), that social media differs according to the user's way. According to Boyd & Ellison (2010), social media means different things to different people, and knotting it into a specific concept has become difficult. This inconsistency in concept may be attributed to the swift changes in technology on the social networking system and the content that is traded.

According to Trottier & Fuchs (2014), social media content can be associated with tweets, blogs, and chat messages shared on Facebook, LinkedIn, YouTube, WhatsApp, etc. Others like Jay Rosen as noted by (Trottier & Fuchs, 2014), attribute social media to a participative activity between individuals and their circle of friends within the cyber-domain. Assigning meaning to the concept of social media is the sole derivative of the word "social". What makes the cyber-domain a social platform depends on certain speculative questions, including: "what does it mean to be social?" Are humans perpetual social or only when they interact with other individuals? Getting the right answers to these questions depend on the concept adopted and may identify the aspect of sociality, transmission, and collaboration of ideas (Trottier & Fuchs, 2014).

As reported by Fuchs (2014), all computing systems, web applications, networking platforms, and all other forms of multimedia resources are termed social media because human knowledge can be transmitted via these mediums. The adverse use of social media platforms has jeopardized social interaction among social media users. However, not every social media user permits the direct sharing of information within the cyber domain. Capping these assertions, the cyber-domain can only be certified social when interactions between humans, media platforms, or computing devices interact and vice versa. The social network or social media platform can therefore be accessed and analysed by its ability to integrate technologies that permit users to display and reflect collective values. These values must be readable, and useful for creating links between the users and they must permit the establishment of links promoting cooperation

2.2. Concept of Cybercrime

Cybercrime includes using a computer or computer network, such as the Internet, to commit criminal acts or activities contrary to acceptable processes (Brush et al., 2022). Cybercrime is any type of illegal, unethical, and unauthorized activity in systems that automatically process information or transmit data (Ahmmed, 2016). Cybercrime includes, but is not limited to, email fraud, hacking, distribution of hostile software, extortion, fraud, identity theft, data theft, attacks on services, terrorism, and stalking. Cybercrime can occur anywhere in the world, regardless of geographic location. In Nigeria, cybercrime, also known as Yahoo Yahoo or 419, is a threat to a society whose impact cannot be quantified and this has been a great concern and embarrassment for the country (Supayah & Ibrahim, 2016).

As reported by Punch (2018), "mondaq.com reported on December 3, 2018, that cyberattacks across Nigeria caused losses totalling 649 million United State dollars in 2017. The report, highlighted those financial losses from online banking fraud reached 5.571 billion British pound sterling between 2015 and 2017, mobile payment fraud reached around 350 million British pound sterling in 2017, and ATM fraud reached 5.57 billion British pound sterling in the same year. The Nigerian Communications Commission CEO also said at the Nigerian Bar Association's 2017 Annual Meeting that the country ranked third in the world for electronic crime, just behind the United Kingdom and the United States announced that 91.6 million people in Nigeria have internet access which avails them with ideas on how to commit crime via the internet.

Figure 1, according to S. Inc. (2021), shows the data statistics on social media users as of January 2019.

2.3. Social Media and Cyber-Crime

According to Singh (2018), stated that the report on “Criminal Use of Social Media” by the National White-Collar Crime Centre (NW3C) highlighted that social media has been on rising in the past several years, which has changed the communicational landscape. Social media network sites, such as Twitter, YouTube, Instagram, WhatsApp, Facebook, etc., have active millions of users. Using these networking websites, individuals communicate without delay with one another at the ease of convenience. Social media sites are used by individuals and the public sector to communicate with each other, advertise, and recruitment of new employees.

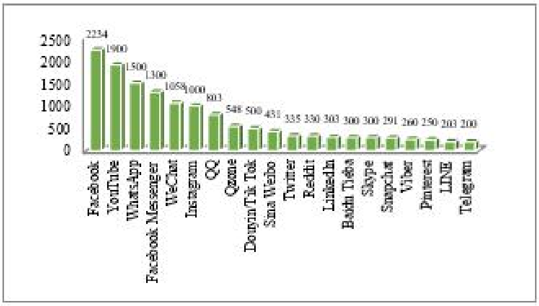

Figure 1. Data statistics on social media users as of January 2019.

Additionally, Andrea (2022), in a publication on information technology industries such as Citizen Lab, Microsoft, and Google during their investigations on zero days (0-days) vulnerabilities highlighted that an enterprise of an Israeli company called Candiru developed a malware known as SOURGUM to exploit vulnerabilities on internet devices and innocent users. Microsoft categorically mentioned that the actor’s spyware is alleged to have been released to attack over 100 victims. It has also been noted that the company had reportedly recruited from the ranks and files of 8200 sets of establishments from the signal’s intelligence unit of the Israeli Defence Forces. They have continued to change their nomenclature bearing the current name as Saito Tech Ltd. The change in nomenclature is to maintain their stealth operations and to continue spying on people's activities.

Phishing is a deceptive means to gaining access to peoples’ devices illegally to exploit essential data such as usernames, passwords, and credit card details via email spoofing and links to topics that appears familiar. Attackers tend to focus more on login credentials when they exploit a vulnerable site or application (Ramzan, 2010). According to Tim (2022), phishing is one of the most common social engineering tools for many cyber attackers. It is easy to launch and achieve success by the perpetrators without any resistance from victims. Most of the time, the victims targeted are customers or clients, and fewer employees of the company, with an ulterior motive to damage the company's reputation, and have their systems compromised.

According to the NW3C report (Trottier & Fuchs, 2014), social media networking service is the most trending online activity globally. The rise of users of internet-enabled PC spends more than 12 minutes per hour on social media networking systems, and as well the number of users of internet-enabled mobile devices has also increased as they spend more than 18 minutes per hour on social media networking systems. With this change in communication methods and durations, criminals are rapidly using social media for malicious purposes. The NW3C report describes six crimes using social media.

Figure 2, according to Sam (2022), shows the statistics of phishing attacks from 2017 – 2020.

2.3.1. Burglary Via Social Networking Sites (SNS)

The intent of every cybercriminal sniffing social media is for potential intrusion, targeting innocent users. Social media users euphorically post personal information and activities such as having fun, having dinner, or when changing location. Cybercriminals delve for such information to spot soft targets and exploit vulnerable social media users.

2.3.2. Social Engineering and Phishing

Social engineering specifically uses psychological manipulation medium to exfiltrate sensitive and personal information from social media users. Social media users usually receive instant messages from pals seeking financial aid. These instant messages originated not from their pals, but rather from criminals who stole their pal's email and password for criminal intent. The simplicity of this method made the cybersecurity organization Trend Micro to call Facebook now Meta "a fraud minefield." An article by Symantec Corporation described phishing as one of the most noted social engineering techniques.

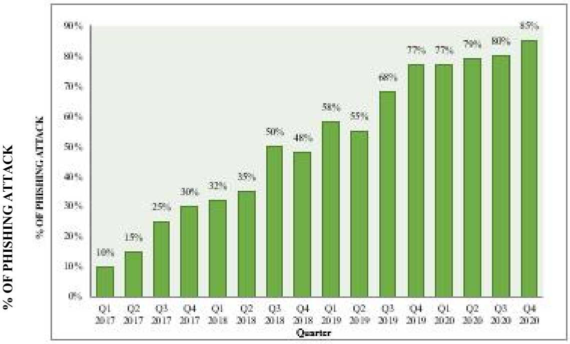

Figure 2. Statistics of Phishing Attacks from 2017 – 2020.

2.3.3. Malware Attack

Social media has been proven to be an excellent medium by which the distribution of viruses, adware, and malware occurs. Developers create and hide their destructive programs in links, attachments, and messages. This happens most often on social networking sites and when users erroneously click on a malicious link, malware is transferred to their computers without their knowledge. Sophos Antivirus developers reported that 40% of their users were analytically noted to be victims of malware via social media. Microsoft also emphasized that 19 million PCs were discovered to be infected with viruses. Likewise, the business community views the use of social media by employees as a network security risk and this made Sophos company survey over 500 companies and over 70% of them were discovered to be more concerned about network security (Singh, 2018).

2.3.4. Identity Theft

Identify theft is an impersonation used to obtain personal information from individuals for criminal intentions. Research suggests that identity theft is the intentional use of a victim's personal information for criminal purposes without legal authority (Dadkhah et al., 2018). According to the Internet Crime Report 2016 as highlighted by the FBI's Internet Crime Complaint Centre (IC3), identity theft rise to 7th position with 16,878 victims, and the United States was the only country to record losses of 58,917,398 United State dollars. In 2017 Internet Crime Report, reported that identity theft was the sixth largest complaint in the United States alone in 2017 with 17,636 victims and a loss of about 66,815,298 million United State dollars (FBI, 2021). Other types of identity theft are credit card fraud, government documents or benefits fraud, loan or lease fraud, bank fraud, employment or tax-related fraud, and phone or utilities fraud (McAfee, 2022). Figure 3, according to McAfee (2022), shows most reported types of identity theft as at 2021.

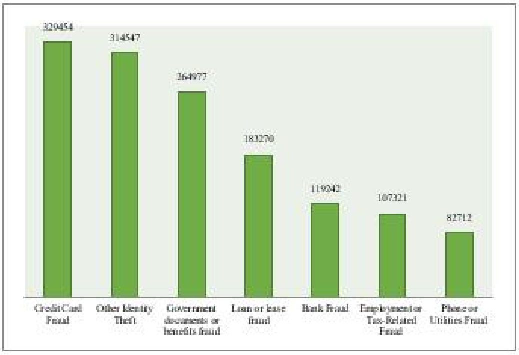

Figure 3. Most reported types of identity theft as at 2021.

2.3.5. Cyber-stalking

Harassment in public using social media or any other online media, which can cause discomfort, abuse, and emotional anxiety in the victim, is termed cyberstalking. The NW3C's Cyberstalking Report further emphasized that cyberstalking is different from identity theft. The report indicates that identity thieves are not concerned with the effect of their actions on their victims, while cyber stalkers are well aware and wilful to do so (Collins et al., 2011). IntelliPaat (2022), highlighted the common attributes of Cyberstalking are tracking locations, breaching data privacy, monitoring both online and real-world activities, obsessively tracking the victims' whereabouts, intimidating victims, etc. Social media stalking may include sending threatening private messages or faking photos.

2.3.6. Cyber-casing

The Social network crime report by the National White-Collar Centre described cyber-casing as a process used to geo-locate the real-world locality of an online user using resources such as individual data uploaded online. One of the main features offered by social media networks recently is geolocation. With the widespread use of mobile apps, geolocation is a major trend on social networking sites. Mobile apps have played an important role in driving this trend, even without a legitimate purpose. Geographic information is the most important factor in the process of accessing a network that can help criminals create malicious plans (Golbeck & Klavans, 2015).

2.4. Routine Activity Theory (RAT)

This is a theory of Marcus Felson and

Lawrence E. Cohen in 1974, which focuses on environmental "criminal opportunities". Essentially, when a potential criminal opportunity presents itself, the behavior occurs at the intersection of time and space between a motivated offender and a suitable target for victimization. This crime will eventually occur in a location where there is no guardian capable of protecting the "suitable target", who is considered a vulnerable person or their unprotected properties Thus, theoretically, the absence of any of these three situational factors would make the commission of a crime impossible (Kitteringham & Fennelly, 2020). Thus, operations theory is often considered a macro-level theory that applies to many types of crime because it seeks to explain the process of becoming a victim of crime, not the specific motive of the crime (Collins et al., 2011). The theory predicts that crime occurs when a motivated offender is exposed to an appropriate target in the absence of a guardian capable of preventing the offender from committing the crime, the theory suggests that the variation in crime rates can be explained by the provision of suitable targets and competent guardians and by their understanding (Ngo & Paternoster, 2011). This theory is agnostic to the role of providing motivated offenders, based on human exploitation, the RAT is applied in this study.

2.5. Existing Resilience Techniques

The use of social media has been an avenue to express individual thoughts on issues dealing with socio-economic, share events of individual lifestyles, and interact with one another (Soomro & Hussain, 2019). The innovation of modern technologies has made cybercriminals to exploit online users' vulnerable data, at the same time post it on social media in text, video, and image form. The same modern social media technology tools used by cybercriminals to perpetrate cybercrime will also be used to control, prevent, protect and investigate cybercrime (Surette, 2015). The routine use of social media in every sector of life has changed individuals' perspectives of viewing cybercrime as well as victimization (McGovern & Milivojevic, 2016). Traditionally, individual users share information and communicate with one another using radio, television as well as newspaper resources. The trend of social media is a pivot in the present communication era, giving an edge to individuals to share incidents happening within their social life, which might aid in nabbing cybercriminals (S. Schneider, 2016).

2.5.1. Combating Burglary

Social media usage can be either positive or negative depending on the user's intent. Cybercriminals always take advantage of available online resources to search for the potential vulnerabilities of other online users and target their victims. Likewise, law enforcement agencies use the same social media to counter the activities of cybercriminals in other to apprehend them (Weir et al., 2011). The operatives of the Economic and Financial Crimes Commission (EFCC) Port Harcourt, Rivers State Zonal Command in Nigeria arrested 74 internet fraudsters through social media resources precisely open source intelligence, this is an example of social media efficiency (Ibunge, 2022). Individuals, executives, as well as corporate organizations, should be wary while using social media. Meticulously examine the type of personal information before sharing, as such information can be used negatively to their detriment noting that everything shared online has a digital signature of the user (Weir et al., 2011).

2.5.2. Combating Social Engineering and Phishing

Social engineers with the intent of white hacking, gray hacking, or black hacking introduce new techniques of social engineering. With this development, online users are encouraged to imbibe the culture of keeping pace by using updated anti-phishing techniques and constantly sorting for the newest countermeasures (Rajab, 2018). According to Aleroud & Zhou, (2017); Singh, (2018), phishing techniques employed by social engineers varies, such include deceptive phishing, malware-based phishing, SMiShing, vishing, cross-site scripting (XSS) and key loggers, etc. Every new innovative phishing technique always has its tools for countermeasures as well.

Further studies by Aleroud & Zhou (2017); Singh, (2018), highlighted less complicated anti-phishing techniques such as one-time passwords (OTP), CAPTCHAs, digital certificates, genetic and characteristics-based anti-phishing processes. However, no anti-phishing mitigating techniques are completely free from phishing. The smartness of social engineers has paved an outstanding way for them to have a stress free to clone social network sites, which without a careful look, might not spot the difference between legitimate and illegitimate sites. The most targeted sites for cloning are financial institutions, reservation sites, humanitarian sites, etc. They generate lots of emails and disseminate them to their victims in anticipation that they will click the attached links in other to exploit their vulnerable data (Rajab, 2018).

Text-based phishing gives room to social engineers to employ various media techniques, mostly social media platforms, as well as other messaging mediums to lure their prey (Jain & Gupta, 2022; Thakur et al., 2018). Natural Language Processing (NLP) has been evaluated as one of the best countermeasure techniques (anti-phishing) against phishing, The integration of NLP automatically analyses the text of an email to assess the threat attributed to it (Khan et. al., 2021).

2.5.3. Combating Malware Attack

There are numerous means by which malware can infect PCs but the easiest means is email link (Kaspersky, 2022). An unsolicited and suspicious email from a financial institution or a pal, mandating you to open a link, is no doubt a malware attempt. Being able to observe and spot illegitimacy is the first line of defence against malware. However, being observant is not full assurance that your computer or network infrastructure is secured; it requires more effort from a more fortified layer such as an antivirus to strengthen your observance.

Further research by He et al. (2015) explored the security risk and threat assessment of smartphones. The studies emphasized that robust Personally Identifiable Information (PII) is being exfiltrated, open-source environment and lack of user awareness posed a great danger to smartphones rendering them vulnerable to a security breach. According to (Sihag et al., 2021), malware is a great threat to individuals, corporate organizations, and nations' technology at large. As such malware developers integrate multiple techniques such as code obfuscation, packaging, and encryption to eschew static analysis (signature-based) and dynamic analysis (behaviour-based) detection methods, the researchers also suggested that the use of the Hardening Mechanism while developing anti-malware should be integrated as well to counter malware.

Additionally, Feng et al. (2021) added that only trusted applications (apps) from reputable and official markets such as Google Play Store and apple store should be patronized, apps from unofficial markets and third-party resources always pose risk and have been a source of serious security breaches to end-users and same must be discouraged.

2.5.4. Combating Identity Theft

Identity theft has been one of the most common means of stealing people's information and protecting the information should be paramount to all individual and corporate organizations: identity owner, identity issuer, identity protector, and identity checker (Wang et al., 2006). Analysing the conceptual framework to detect, identify and prevent identity theft should involve all the stockholders with their roles and responsibility. Personal identity is often called PII, which is contained in an identity document such as health care records, birth document, or international passport and it is the responsibility of the identity bearer to protect it after being issued by the issuing authority (Ji et al., 2008).

According to Hedayati (2012), opined that individuals and corporate organizations should routinely adhere to timely checks of their financial details including transactions, avoid moving about with sensitive identity documents, and as well be wary of sharing PII with unknown individuals. Another researcher (EL-Sakran, 2019), stated that issuing authorities should always be contacted for certificate verification, especially on suspicion of educational identity theft. Negligence of this magnitude may pose serious and irreparable reputational damage to the organization and its stakeholders.

2.5.5. Combating Cyber-Stalking

The innovation of modern technology is not only beneficial to society but also has well created an adverse impact. To curb this adverse impact, be mindful of posting personal data on Social Media Accounts, regularly conduct Internet reconnaissance for your identity, be mindful of your passwords, being wary of unsolicited emails, texts, and phone calls that seek your PII, routine change of all account security when quitting relationship and seek expert help upon discovery of being cyberstalked (Darrin, 2017). As technology advances, harassment has also been upgraded in the cyber domain.

According to Steve (2019) defined cyberstalking as online stalking involving the repeated use of internet platforms such as email, instant messages, phone calls, and other communication means to harass, intimidate or cause fear to an individual or an organization. Cyberstalks use false accusations or upload defamatory statements, monitor someone's online activity or geolocation, and cause threats, identity theft, as well as data destruction or manipulation by sending malware to a target's devices. The researcher suggested that social media users should adhere to the following techniques; do not allow physical access to their PCs and web-enabled devices like smartphones, cultivate the habit of logging out of PC programs when not in use, restrict screensaver with a password, practice good password management using Password Managers Account and online account security, important online calendars or itineraries should either be deleted or made private and use a trusted security software program such as Norton 360 with LifeLoc, QuickHeal Total Security for smartphones to help prevent spyware from being installed onto your internet-enabled devices through a phishing attack or an infected web page.

2.5.6. Combating Cyber-Casing

Reservations booked via social media handles contribute to the exposure of sensitive data to cybercriminals while cyber-casing. Social media users euphorically geotag their pictures, text, videos, etc., without the knowledge that it is potentially risky. It is the easiest means for cybercriminals to exploit personally indefinable information for nefarious intent. However, techniques such as switching off your location services on your smart devices when not in use, neither updates about your location, or pictures while on vacation nor publicly communicating time to be home online (Alex, 2013).

Further research by Friedland & Sommer (2010) emphasized that inculcating online users about the consequences of geotagging, will broaden their know-how and at the same time arm them with the authority to make informed decisions.

3. Research Methodology

3.1. Research Design

The study used both qualitative and quantitative research design that was gathered from secondary and primary sources of data.

3.2. Population of the Study

The population of the study will be the total number of social media users in Abuja Nigeria. An estimated 7, 110,000 (Seven million, one hundred and ten thousand) social media users in Abuja will be used for the study (Nairametrics, 2022).

3.3. Sample Size and Sampling Techniques

The sample size for the study was determined by using Taro Yamane's purposive sampling technique (Yamane, 1967). The formula used is;

$$n = \frac{N}{1+N(e)^2} \qquad (1)$$

where n= sample size sought, N= given Population = 7, 110,000, e= level of significance (Reliability) = 0.05

$$n = \frac{7,110,000}{1+7,110,000\ (0.05)^2}$$

$$n = \frac{7,110,000}{17,775.0025}$$

$$n = 399.99 \sim 400$$

Therefore, the sample size for the study was 400 respondents who were selected using Taro Yamane's purposive sampling technique.

3.4. Sources of Data

Primary and secondary sources of data were used for this study. The primary source of data is a questionnaire titled: Ph.D. Questionnaire while the secondary sources include data from journals and articles.

3.5. Method of Data Analysis

Data collated from the questionnaire were analysed using mean and standard deviation with the five-point modified Likert response rating scale reaching from Strongly Agree (5 points), Agree (4 points), Neutral (3 points) Disagree (2 points), and Strongly Disagree (1 point) as opined by Ahmad et al. (2021); Jebb et al. (2021).

4. Data Presentation, Analysis, and Discussion of Findings

4.1. Demographic Data Presentation

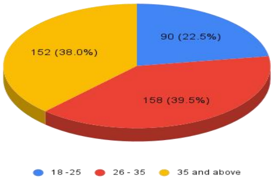

Figure 4. Age range of respondents, number of respondents, and percentage. Figure 4 revealed that the age range of 26-35 is dominant with 39.5% of the 400 respondents used for the study.

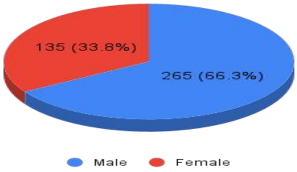

Figure 5. Gender of respondents, number of respondents, and percentage.

Figure 5 shows that there are more male respondents with 66.3% of the 400 respondents selected for the study.

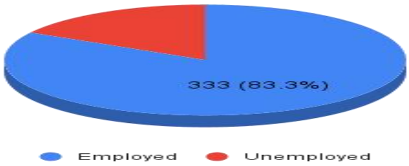

Figure 6. Employment status

Figure 6 indicates that there are more employed respondents with 83.3% of the 400 respondents selected for the study.

4.2. Data Presentation and Analysis

In this section, the data collected for the study were analysed to provide answers to the research questions that guided the study.

Research Question One: What are the various cybercrimes perpetrated by cyber attackers on social media users?

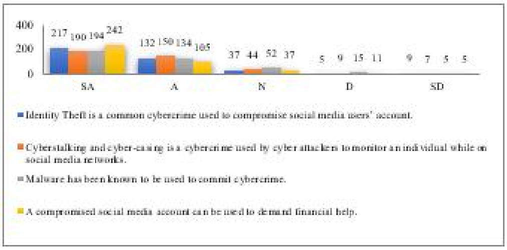

Figure 7. Number of respondents to the various cybercrimes perpetrated by cyber attackers on social media users.

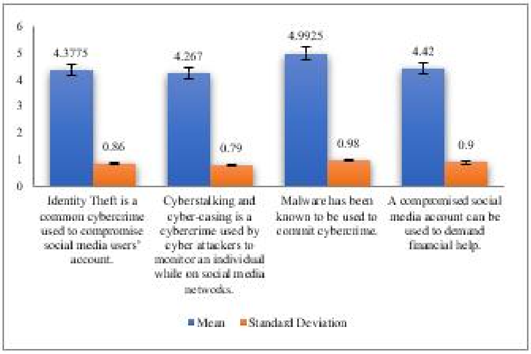

Figure 8. Mean and standard deviation of respondents on the various cybercrimes perpetrated by cyber attackers on social media users.

The Figures (7 and 8) show the appraisals of the respondents on the various cybercrimes perpetrated by cyber attackers on social media users. From the Figures (7 and 8), it was shown that identity theft, online stalking, malware attack, and cyber-casing are major cybercrimes perpetrated online by cyber attackers. The stated items had been universal with a criterion mean greater than 4.0 suggesting that all the respondents agree with the statements.

These results correlate with (Symantec, 2019), where it was found that Microsoft corporation reported that 19 million PCs were infected with malware. Additionally, the business community considers the use of social media networks by their employees as a cybersecurity risk. Sophos surveyed more than 500 companies and 70% of them were concerned about cybersecurity due to their employees' use of social media. Cybercriminals use various methods to gather information about their potential targets through social engineering techniques. Phishing emails can be similar to a boss asking an employee for the individual's login or banking information. Cybercriminals are sure to scare their targets by following instructions rather than thinking rationally. Criminals use this method to send millions of emails in anticipation of getting and exploiting vulnerable information. The most known form of scam is to create a page similar to Facebook or a bank. According to the (FBI, 2021), criminals often set up bogus charities after a natural disaster and illegally gain from individuals who believe they are contributing to the lives of disaster victims. IC3's 2017 report found a total of 436 disaster fraud victims, costing 1,405,460 million United States dollars in United States, and the Consumer Networks Security (CSN) 2017 data book described it as a mild but gradual and continuous increase in disaster fraud. CSN statistics show 3,174, 3,483, and 3,703 complaints filed in 2015, 2016, and 2017.

A scholar further opined that preventing email compromise requires sending domains to enable the protocols for the receivers to verify that emails are originally generated by the sender's domain. It is a vice versa method involving both the sender and receiver enabling their protocols which involve Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC), (Roger A. Grimes, 2019).

Research Question Two: What are the impacts of cybercrimes on social media users?

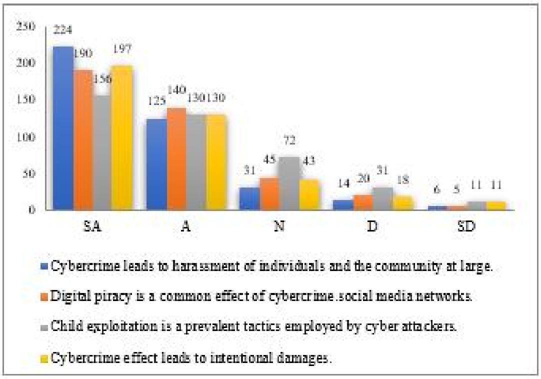

Figure 9. Number of respondents on the impact of cybercrimes on social media users.

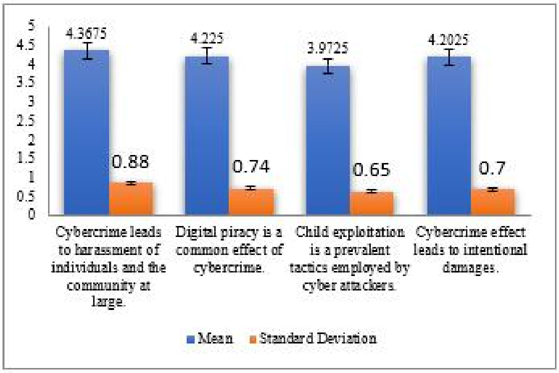

Figure 10. Mean and standard deviation of respondents on the impacts of cybercrimes on social media users.

Figure 9 and 10 present the responses of the respondents on the impacts of cybercrimes on social media users. All the items stated show that the impacts were all accepted with a criterion mean greater than 3.9. The table discloses that social media cybercrime has an impact on its victims as it has led to harassment, child exploitation, digital piracy, and intentional damage to individuals' online reputations. These results coincide with research by Martellozzo et al. (2010), in which they reiterated that the impact of a successful cyber-attack can have far-reaching implications including financial loss, theft of intellectual property, and loss of consumer trust. The risks children take when they are online are many, exposure to inappropriate conversation; accidentally becoming the subject of a sexual fantasy; receiving indecent or sexually explicit images; being asked to submit indecent pictures of themselves or their friends; engaging in an erotic conversation, and are encouraged to perform sexually explicit acts against themselves or their friends.

According to Cleary (2019), who highlighted that in the International Federation of recording Industries -IFPI Digital Music Report of 2015, the music industry saw a 31% drop in sales between 2004 and 2010. One of the potential causes of the loss is digital piracy, which is said to be very expensive for the music industry, costing 28.3 billion dollars a year. The sum of 20 billion United States dollars was incurred as a loss by the film industry and 8.3 billion United States dollars from the software industry in 2010 by International Data Corporation. The most fundamental cybersecurity measures in securing a business from a cyberattack are knowing and understanding vulnerabilities within, weighing the potential risk, and carefully choosing the best tools for securing your business. The application of the strong form of multi-factor authentication (MFA) and authentication standards such as Fast Identity Online v2 (FIDO2) or Web Authentication (WebAuthn) and Modern authentication strategies such as risk-based authentication and Security Assertion Markup Language (SAML) will contribute immensely in securing network sites (Tim, 2022).

Research Question Three: What are the various individual resilience techniques used by social media users to combat cybercrimes?

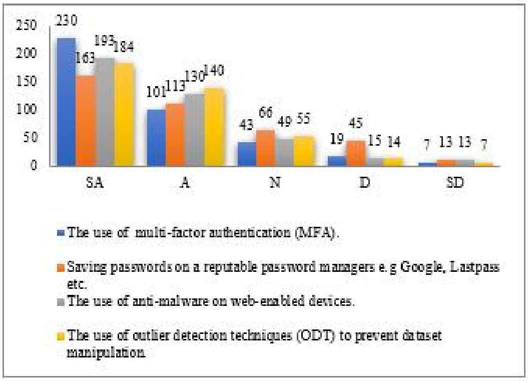

Figure 11. The various individual resilience techniques used by social media users to combat cybercrimes.

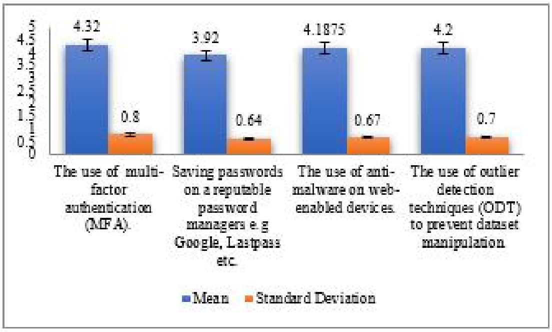

Figure 12. Mean and standard deviation of the various individual resilience techniques used by social media users to combat cybercrimes.

Figure 11 and 12 assessed the response of the respondents on various individual resilience techniques used by social media users to combat cybercrimes. With a criterion mean of 3.9 and above, all the statements were accepted. Decisively, the study revealed that the use of anti-malware, outlier detection, password managers, and MFA are various individual resilience techniques social media users can employ in combatting cybercrime on social media. These results correlate with the findings of Feng et al. (2021); Mshana (2015), who stated that a way to prevent cybercrime is through the use of reliable open-source software. Reliable open-source software allows users to self-assess security or hire a party of their choice to perform security assessments for them. The open-source software even allows different, independent groups of people to assess the security of a system, eliminating the reliance on a single party to decide for or against a given system. According to another study by Gunter et al. (2010), believe that the safest way to protect individual account IDs is to use other software such as Google Authenticator. This process involves changing a one-time numeric password when attempting to register from an unknown location. Without this unique password, registration becomes a problem for the scammer and the account will remain intact. To increase the counter threat posed by cyberattacks, the use of two-factor authentication is necessary while login on any online platform. Then securing an email enrouting Simple Mail Transmission Protocol (SMTP) for authentication requires techniques such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Domain Keys Identified Mail (DKIM) and Sender ID, especially for information technology savvier and organizations. These techniques will increase restrictions on email address spoofing when an unauthorized access is attempted (Ramzan, 2010).

5. Conclusion and Recommendations

The study aims to combat cybercrime perpetrated via social media channels using individual resilience techniques. From the analysis carried out in this research work, it revealed that;

1. Identity theft, cyber stalking, malware attack, and cyber-casing are the major cybercrimes perpetrated online by cyber attackers.
2. Cybercrime has led to harassment, child exploitation, digital piracy, and intentional damage to individuals' online reputations.
3. The use of anti-malware, outlier detection, password managers, and MFA are various individual resilience techniques social media users can employ in combatting cybercrime on social media.

Social media is a great platform for anyone sourcing for a prospective buyer of products or services, or employees for specific designations, and an ideal target for affiliates of crimes such as identity theft, cyberstalking, cyber-casing, etc. The impact of cybercrime on social networks society has become unsustainable, amid the global economic crisis. It is necessary to work together to avoid unnecessary costs as the risk of business collapse is real, given the high costs of mitigating measures and the damage caused by countless attacks.

The mitigation of this heinous crime also depends on the attitude and character of each individual. Before protecting the wider society, every social media user that can be hacked should be security conscious and protect their social media account as it contains other details about their people. Applying different individual resilience techniques will not only protect you personally, but also your friends, family, and acquaintances.

However, the study was also faced with the following limitations:

1. Access to sensitive data and data privacy

2. Dynamic nature of social media platforms in regards to evolving features, policies, and user behaviours.
3. Underreporting and lack of standardized metrics for cybercrime incidents on social media

Finally, from the findings of this study, it recommended that:

1. More awareness should be created and publicized about the presence of cybercrime and the various techniques used to exploit individuals, and organizations.
2. The government should set up a special task force void of bias to help cybercrime victims regain their assets, image, and emotional states after any cyberattack.
3. Every social media user should select a unique technique for protecting his/her social media accounts on web-enabled devices especially using MFA.

References

AbdulRaheem, M., Misra, S., Awotunde, J.B., Oladipo, I.D., Oluranti, J. (2022). Automated Fingerprint Biometric System for Crime Record Management. In: Abraham, A., et al. Innovations in Bio-Inspired Computing and Applications. IBICA 2021. Lecture Notes in Networks and Systems, vol 419. Springer, Cham. https://doi.org/10.1007/978-3-030-96299-9_76.

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, *9*, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383.

Adesola, F., Misra, S., Omoregbe, N., Damasevicius, R., Maskeliunas, R. (2019). An IOT-Based Architecture for Crime Management in Nigeria. In: Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G. (eds) Data, Engineering and Applications. Springer, Singapore. https://doi.org/10.1007/978-981-13-6351-1_19.

Adesola, F., Azeta, A., Misra, S., Oni, A., Ahuja, R., Omolola, A. (2022a). Analysis of Violent Crime Dataset Using Support Vector Machine Model. In: Singh, P.K., Kolekar, M.H., Tanwar, S., Wierzchoń, S.T., Bhatnagar, R.K. (eds) Emerging Technologies for Computing, Communication and Smart Cities. Lecture Notes in Electrical Engineering, vol 875. Springer, Singapore. https://doi.org/10.1007/978-981-19-0284-0_15.

Adesola, F., Azeta, A., Misra, S., Oni, A., Ahuja, R., Omolola, A. (2022b). Spatial Analysis of Violent Crime Dataset Using Machine Learning. In: Singh, P.K., Kolekar, M.H., Tanwar, S., Wierzchoń, S.T., Bhatnagar, R.K. (eds) Emerging Technologies for Computing, Communication and Smart Cities. Lecture Notes in Electrical Engineering, vol 875. Springer, Singapore. https://doi.org/10.1007/978-981-19-0284-0_14.

Ahmad, A. R., Alhammad, A. H. Y., & Jameel, A. S. (2021). National Culture , Leadership Styles and Job Satisfaction : An Empirical Study in the United Arab Emirates. *Journal of Asian Finance, Economics and Business*, *8*(6).

https://doi.org/10.13106/jafeb.2021.vol8.no6.1111

Ahmmed, F. (2016). Meaning and Nature of Cyber Crime. *Academia*. https://www.academia.edu/41411512/Meaning_and_Nature_of_Cyber_Crime

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00047-5

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. In *Computers and Security* (Vol. 68). https://doi.org/10.1016/j.cose.2017.04.006

Alex, M.-M. (2013). *Cybercasing – How Sharing Your Pics, Videos and Status Updates Can Get You Into Trouble | McAfee Blog*. McAfee. https://www.mcafee.com/blogs/family-safety/cybercasing-how-sharing-your-pics-videos-and-status-updates-can-get-you-into-trouble/

Althukair, A., Al Johi, H., Alkhaldi, N., & Al Zahrani, J. (2021). The Role 0f Social Media In Health Seeking Behavior Of Patients Attending Primary Health Care Setting At National Guard, Dammam, Saudi Arabia. *International Journal of Scientific ResearCH*. https://doi.org/10.36106/ijsr/0934390

Andrea, P. (2022). *Report: Mercenary spyware exploited Google Chrome zero-day to target journalists - The Record by Recorded Future*. The Rcord by Recorded Future. https://therecord.media/report-mercenary-spyware-exploited-google-chrome-zero-day-to-target-journalists/

Argus, N. (2004). *Jane "murdered in sex fantasy."* The Argus.

Asanga, M.P., Essiet, U.U., Ukhurebor, K.E., Afolorunso, A., Hussaini, P. (2023). Social Media and Academic Performance: A Survey Research of Senior Secondary School Students in Uyo, Nigeria. International Journal of Learning, Teaching and Educational Research, 22(2), 323-337.

Awari, G. K., & Warjurkar, S. V. (2022). Computer and Internet Crime. In *Ethics in Information Technology*. https://doi.org/10.1201/9781003280989-2

Brush, K., Rosencrance, L., & Cobb, M. (2022). Cybercrime-What is cybercrime? *TechTarget-SearchSecurity*.

Chawki, M. (2005). Computer Crime Research Center. *Computer Crime Research Center*.

Cleary, M. (2019). IFPI Digital Music Report 2015. *Journal of Chemical Information and Modeling*, *53*(9).

Collins, J. D., Sainato, V., & Khey, D. N. (2011). Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. *International Journal of Cyber Criminology*, *5*(July).

Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). Identity Theft in the Academic World Leads to Junk Science. *Science and Engineering Ethics*, *24*(1). https://doi.org/10.1007/s11948-016-9867-x

Darrin. (2017). *6 Ways to Avoid Becoming a Cyberstalking Victim | NAI*. North American Investigations. https://pvteyes.com/6-ways-avoid-cyberstalking-victim/

EL-Sakran, T. M. (2019). Educational tips for the detection of resume padding. *Journal* *of Pedagogical Innovations*, *7(2)*.

Emeka, E.P., Okoza, J., Ukhurebor, K.E., Onwodi, G.O., Bayonle, F., Nyagblordjro, J. (2023). The Impact of Internet Use on Tertiary Institution Students' Academic Performance: An Exploratory Study. Cypriot Journal of Educational Sciences, 18(1), 253-267.

Et. al., M. T. H. F. K. (2021). Detecting Phishing Attacks using NLP. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2). https://doi.org/10.17762/turcomat.v12i2.816

FBI. (2021). FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics. *News*.

Feng, R., Chen, S., Xie, X., Meng, G., Lin, S. W., & Liu, Y. (2021). A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices. *IEEE Transactions on Information Forensics and Security*, *16*. https://doi.org/10.1109/TIFS.2020.3025436

Friedland, G., & Sommer, R. (2010). Cybercasing the joint: On the privacy implications of geo-tagging. *HotSec 2010 - 5th USENIX Workshop on Hot Topics in Security*.

Golbeck, J., & Klavans, J. L. (2015). Introduction to Social Media Investigation: A Hands-on Approach. In *Introduction to Social Media Investigation: A Hands-on Approach*. https://doi.org/10.1016/C2014-0-01104-5

Granados, N. (2016). *What Is Media In The Digital Age?* Forbes. https://www.forbes.com/sites/nelsongranados/2016/10/03/what-is-media-in-the-digital-age/?sh=7bd50fbe51ea

Gunter, W. D., Higgins, G. E., & Gealt, R. E. (2010). Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents. *International Journal of Cyber Criminology*, *4*(1).

He, D., Chan, S., & Guizani, M. (2015). Mobile application security: Malware threats and defenses. *IEEE Wireless Communications*, *22*(1). https://doi.org/10.1109/MWC.2015.7054729

Hedayati, A. (2012). An analysis of identity theft : Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution*, *4*(January).

Hinduja, S., & Schafer, J. A. (2009). US cybercrime units on the world wide web. *Policing*, *32*(2). https://doi.org/10.1108/13639510910958181

Ibunge, B. (2022). *EFCC Arrests 74 Suspects for Internet Fraud in Rivers – THISDAYLIVE*. This Day News. https://www.thisdaylive.com/index.php/2022/07/25/efcc-arrests-74-suspects-for-internet-fraud-in-rivers/

IntelliPaat. (2022). *What is Cyberstalking and How to Protect Yourself?* Intelli Paat. https://intellipaat.com/blog/what-is-cyberstalking/

Isah, A.O., Alhassan, J.K., Misra, S., Idris, I., Crawford, B., Soto, R. (2016). Network System Design for Combating Cybercrime in Nigeria. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2016. ICCSA 2016. Lecture Notes in Computer Science, vol 790. Springer, Cham. https://doi.org/10.1007/978-3-319-42092-9_38.

Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. In *Enterprise Information Systems* (Vol. 16, Issue 4). https://doi.org/10.1080/17517575.2021.1896786

Jebb, A. T., Ng, V., & Tay, L. (2021). A Review of Key Likert Scale Development Advances: 1995–2019. In *Frontiers in Psychology* (Vol. 12). https://doi.org/10.3389/fpsyg.2021.637547

Ji, S., Chao, S. S., & Min, Q.-F. (2008). Systems Plan for Combating Identity Theft – A Theoretical Framework. *Journal of Service Science and Management*, *01*(02). https://doi.org/10.4236/jssm.2008.12015

Josh, F. (2020). *Marriott data breach FAQ: How did it happen and what was the impact?* https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Kaspersky. (n.d.). *What is Malware, and How to Protect Against It?* Kaspersky. Retrieved October 10, 2022, from https://www.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Kawasaki, G., & Fitzpatrick, P. (2013). The Art of Social Media. Power tips for power users. In *New Zealand Apparel* (Vol. 46, Issue 2).

Kitteringham, G., & Fennelly, L. J. (2020). Environmental crime control. *Handbook of Loss Prevention and Crime Prevention*, 207–222. https://doi.org/10.1016/B978-0-12-817273-5.00019-3

Martellozzo, E., Nehring, D., & Taylor, H. (2010). Online child sexual abuse by female offenders: an exploratory study. *International Journal of Cyber Criminology*, *4*(July).

McAfee. (2022). *A Guide to Identity Theft Statistics for 2022 | McAfee Blog*. McAFee. https://www.mcafee.com/blogs/tips-tricks/a-guide-to-identity-theft-statistics-for-2022/

McGovern, A., & Milivojevic, S. (2016). Social media and crime: the good, the bad and the ugly. *The Conversation*, *March*.

Mshana, J. A. (2015). Cybercrime: an empirical study of its impact in the society: a case study of Tanzania. *Huria: Journal of the Open University of Tanzania*, *19*(1).

Murtaza, M. R., Siddiqi, A., Mugheri, M. A., & Kanwal Oad, M. S. (2017). Advanced Persistent Threats Defense Techniques: A Review. *Pakistan Journal of Computer and Information Systems*, *2*(2), 53–65. http://pastic.gov.pk/downloads/PJCIS/PJCIS_V2_2.pdf

Nairametrics, R. T. (2022). *States in Nigeria with largest internet subscribers as of March 2022 - Nairametrics*. Nairametrics. https://nairametrics.com/2022/06/28/states-in-nigeria-with-largest-internet-subscribers-as-of-march-2022/

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber …*, *5*(1).

Nwankwo, W., Ukhurebor, K.E. (2020). Web Forum and Social Media: A Model for Automatic Removal of Fake Media using Multilayered Neural Networks. International Journal of Scientific & Technology Research, 9(1), 4371- 4377.

Odinakachi, E.O., Mbalisi, O.M., Ukhurebor, K.E., Opateye, J., Leonard, E. (2023). Accessibility of Instructional Materials for Effective Teaching: Outlook from High Schools in Eleme, River State, Nigeria. Cypriot Journal of Educational Sciences, 18(2), 456-469.

Olusegun, A.A., Uranta, E., Ukhurebor, K.E., Jokthan, G., Bello, A., Nalwadda, D. (2023). Appraisal of E-Learning and Students' Academic Performance: A Perspective from Secondary Schools. Cypriot Journal of Educational Sciences, 18(1), 351-367.

Omoregbe, N., Misra, S., Maskeliunas, R., Damasevicius, R., Falade, A., Adewumi, A. (2019). Design and Implementation of an E-Policing System to Report Crimes in Nigeria. In: Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G. (eds) Data, Engineering and Applications. Springer, Singapore. https://doi.org/10.1007/978-981-13-6351-1_21.

Punch, N. (2018). *Central Bank of Nigeria issues guidelines to combat rising financial cybercrime - Punch Newspapers*. Central Bank of Nigeria Issues Guidelines to Combat Rising Financial Cybercrime. https://punchng.com/central-bank-of-nigeria-issues-guidelines-to-combat-rising-financial-cybercrime/

Rajab, M. (2018). An anti-phishing method based on feature analysis. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3184066.3184082

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. In *Handbook of Information and Communication Security*. https://doi.org/10.1007/978-3-642-04117-4_23

Roger A. Grimes. (2019). *Preventing address spoofing with DMARC, DKIM and SPF*. https://www.csoonline.com/article/3402016/3-email-security-protocols-that-help-prevent-address-spoofing-how-to-use-them.html

S. Inc. (2021). "Number of social media users worldwide from 2010 to 2021 (in billions),." *Statista: The Statistics Portal, New York, 2019.*

S. Schneider. (2016). Hoffman Estates family turns to Facebook to help identify home burglars. *Fox 32 Chicago*.

Sam, C. (2022). *Phishing statistics and facts for 2019–2022 | Comparitech*. Comparitech. https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

Scott, F. (2021, July). *Saudi Aramco Traces Data Leak to Attack on Supplier*. https://www.bankinfosecurity.com/saudi-aramco-says-supplier-leaked-company-data-a-17130

Sharma, T., & Bashir, M. (2020). An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited. *Advances in Intelligent Systems and Computing, 1219 AISC*. https://doi.org/10.1007/978-3-030-52581-1_7

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12*(12), 6042. https://doi.org/10.3390/app12126042

Sihag, V., Vardhan, M., & Singh, P. (2021). A survey of android application and malware hardening. In *Computer Science Review* (Vol. 39). https://doi.org/10.1016/j.cosrev.2021.100365

Singh, L. J. (2018). A Survey on Phishing and Anti-Phishing Techniques. *International Journal of Computer Science Trends and Technology (IJCST)*, *6*(2).

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*, *24*(1). https://doi.org/10.2478/acss-2019-0002

Statista. (2020). Number of social media users worldwide from 2010 to 2021 (in billions). In *The Statistics Portal*.

Steve, S. (2019). *Cyberstalking: Help protect yourself against cyberstalking | Norton*. Norton Life Lock. https://us.norton.com/blog/how-to/how-to-protect-yourself-from-cyberstalkers#

Supayah, G., & Ibrahim, J. (2016). An Overview of Cyber Security in Malaysia. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *6*(4). https://doi.org/10.12816/0036698

Surette, R. (2015). How social media is changing the way people commit crimes and police fight them. *London School of Economics*.

Symantec, C. (2019). Internet Security Threat Report. *Network Security*, *24*(February).

Thakur, K., Shan, J., & Pathan, A. S. K. (2018). Innovations of phishing defense: The mechanism, measurement and defense strategies. *International Journal of Communication Networks and Information Security*, *10*(1). https://doi.org/10.17762/ijcnis.v10i1.2991

Tim, F. (2022). *10 top anti-phishing tools and services*. https://www.csoonline.com/article/3575080/9-top-anti-phishing-tools-and-services.html

Trottier, D., & Fuchs, C. (2014). Theorising social media, politics and the state: An introduction. In *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, *22*(1–2). https://doi.org/10.1080/13600860801924907

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. *IEEE Security and Privacy*, *4*(2). https://doi.org/10.1109/MSP.2006.31

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, *16*(2). https://doi.org/10.1016/j.istr.2011.09.008

Yamane, T. (1967). Statistics: An Introductory Analysis, 2nd Ed., New York: Harper and Row. In *Journal of Agricultural Extension and Rural Development* (Vol. 11, Issue 2).