Social Media and Cyber-Crime Among Abraka Residents, Delta State, Nigeria

Joyce Agbaka
Department of Mass Communication, Faculty of Social Sciences,
Delta State University, Abraka, Nigeria
E-mail: agbakaj@gmail.com

Abstract

Social media platforms have become a routine for many people. The number of active social media users have more than doubled within a couple of years resulting in current record of over one billion. The lack of control of social media have created room for vices, such as fraud, falsehood, sedition, blackmail, pornography, invasion of privacy, and other unacceptable practices. One of the greatest problems affecting social media is that it promotes superficial connection that can end up causing long term emotional and psychological problems. This study was undertaken to determine social media and cyber-crime among Abraka residents. A sample of three hundred (300) respondents were drawn from seven (7) different locations and zones in Abraka, using the simple random sampling technique. The descriptive survey research design was adopted and data was collected from the three hundred (300) questionnaires administered and in-depth interview conducted. Data from questionnaires were analysed using the Statistical Package for the Social Sciences (SPSS) version 21 in order to test the extent to which social media users are aware of the use of social media platforms in the perpetuation of cyber-crime. The results revealed that social media platforms such as Whatsapp, Facebook, Twitter, Youtube, Badoo, Instagram, BBM, etc have been used to perpetuate cyber-crime. On the basis of these findings, the study concluded that social media-aided cyber-crimes have significant effect on its users and that social media, with its positive impact, have brought serious threats to the society. Based on the findings, the study recommends the use of password codes among social media users in order to restrict leakage of vital/relevant information on the internet from social media users to fraudsters.

Keywords: Social media, cyber-crime, superficial connection

INTRODUCTION

Social media can be regarded as one of the greatest achievements that has occurred to humanity, especially in the area of Mass Communication. However, Boyd and Elisson (2008) and Ellison, Esra and Melissa (2007) say that there is a lack of criminological inquiry into their role in engaging in crime and crime prevention. Amedie (2015) corroborates this, when he noted that social media promotes superficial connection that can end up causing long term emotional and psychological problems. It has been argued in various studies (Long and Chiemeke, 2008; Augustine, 2010; Anderson, 2012; Laura, 2015) that social media and cyber-crime have led to the collapse of most sectors in the Nigerian society. Studies carried out by these authors have also shown that social media and cyber-crime are causing near total collapse of most cities in Nigeria particularly Lagos, Warri, Port-Harcourt, Calabar and Abuja, with over 90% of criminals coming from the social media. The reason for this trend is that it is easier to perpetuate cyber-crime through social media platform.

Oliver (2010) noted that wrong value systems and the desire to get rich quick without working for it are the key factors encouraging cyber-crime in Nigeria. Cyber-crime is complex and committed mostly from remote locations making it difficult to police (Oliver, 2010). Authorship attribution for cyber-crimes and cyber-attacks are also major problems for all law enforcement agencies (Okonigene and Adekanle, 2009). As earlier stated, the internet has a capacity for more good than bad. This is better explained by Moses and Roseline (2012:21) who stated that “The oxymoronic nature of the Internet is one of its unforeseen attributes; at its inception, no one, perhaps, could have clearly foreseen that, and how, the Internet would someday become a veritable platform for globalised criminal activities". Moses and Roseline (2012:28) went further to say that, the benefits of the internet have so often been tainted by its versatility for virtual criminal activities that have vastly devastating physical and social implications. Many will agree that concerns are increasing as Nigeria is increasing its digitalisation not only in the area of commerce and communications, but gradually into the area of electronic banking.

According to Ibikunle and Eweniyi (2013), as the country integrates electronic payment system into its financial institution; a step that is expected to accelerate the nation's e-commerce growth, the negative impact of cyber-crime on businesses, and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the minds of users and potential online users. There is need to focus on a way to reduce or completely eradicate the rise and dangers of cyber-crime and breach in social media platforms in Nigeria (Oliver, 2010). It has been observed that less efforts have been directed towards examining the extent to which social media platforms have been used to perpetuate cyber-crime in Nigeria. Efforts have mainly geared towards ascertaining the positive impact of social media but none have carefully looked at its negative effect on users. It is against this background that this study seeks to examine social media and cyber-crime among Abraka residents with a view to proferring solutions to these problems.

LITERATURE REVIEW

Social Media and Cyber-Crime

Social media is defined as a medium to interact the people to create, share, exchange and commenting contents in networks and virtual communities (Abouharb and Cingranelli, 2007; Okolie et al., 2023). Therefore, the theory of social media (networking) technology is an integrating tool of education that improved national development in the education sector. Social media, an offspring of new media, typify these features as they have eliminated geographical distance in global communication. According to Barsh (2013) three components typify social media: concept (art, information, or meme); media (physical, electronic, or verbal); and social interface (intimate, direct, social viral, electronic broadcast or syndication or print.). According to Esra and Melissa (2017) the popularity of social media has grown expediently. The social networking site such as Facebook, MySpace, Instagram, Badoo, Twitter, and BB chat allows social interaction among students. The study examined the positive effect of such site on youths especially in the advent of cyber-crime and computer hacking. It said, gone are those days when events happen and it stays a while before people begin to hear about it. But now, through social media, events and news are now known within splits second after they are shared. It offers youths a channel for entertainment, communication, and meeting friends and those you've not seen for a long time. However, the negative effects of social media on cyber-crime abounds.

The use of social media platforms has become widespread over the recent years especially in engaging in all forms of criminal activities such as cyber-crimes. For many, the use of these social media platforms has become daily routine, particularly young generations. Social media become an integral part of their socials. According to Barsh (2013) the use of various social media platform has become everyday routine for many people especially in engaging in criminal activities. The number of active social media users has more than doubled in a couple of years being around one million users in 2012 and social media application allows individuals users and organizational users to interact dynamically and share as well as produce using these platforms.

Social Media Platforms

Social media platforms such as Instagram, Badoo, Twitter and Facebook have become essential to free expression in the digital age. From across the Federation of Nigeria, one could see how movements around the world have used internet-based platforms to communicate, organize, and share critical information that impacts their lives (Chauhan, 2004). It is easy to forget that social media platform was created as a simple tool to let college classmates get to know each other. Now that platforms have billions of users, the decisions that social media companies make impact free expression on a global scale. Indeed, many people who are new to the internet tend to confuse social media application with the internet itself, new research by the Mozilla Foundation confirms a fact that has important implications when it comes to free expression (Forsythe, 2010). Social media platforms are where people connect with other people online. As such, police and security agencies, especially in repressive countries, often rely on social media to force people-members of minority groups, journalists, activists, and others-to reveal their social networks. With one password, sometimes revealed under torture, government authorities can clamp down on entire communities (Forsythe, 2010). Most internet hackers have worked with platforms to develop mechanisms to hack relevant details pertaining to ATM pins, follow up in case of kidnapping, money transfer, etc.

Social media platforms have responded over the years by developing numerous positive security enhancements. However, these platforms do not get it right all of the time. For example, Twitter is without a doubt one of the most important platforms for news and information in the 21st century used to protect cyber-crime. The use of social media platforms worldwide has generated a lot of issues relating to cyber-crime and internet theft (Okunna, 1999). As Kaye (2017) observed, “most social media platforms are used in committing crimes and engaging in internet fraud popularly known as “yahoo” Many at-risk users rely on social media platforms to fulfill all three of these important precepts. But when people are forced to reveal their real identity-or an adversary exposes it-their ability to exercise that right is threatened, and in some cases, their lives are placed in danger. This risk will become even more significant as social media platforms position itself to deliver the world’s news (Boyd and Ellison, 2007).

Complexities of Cyber-crime

The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communication networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context. New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner’s permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank (Yar, 2005). The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computational concepts.

Information has several unique and abstract properties, for example its capacity to still be in the owner's possession after it has been copied or stolen (Nojeim, 2009). The last decade has seen the legal system struggle with the implications of this in a computer-based context. Clearly, conventional notions of copyright, patent rights and theft have been strained when applied to software and computer-based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins). A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways-mathematically, by encryption, or by conversion to say a holographic image or a piece of music (Adebusuyi, 2008). As long as the method(s) of transformation are known, the music, image, or encrypted text can be translated back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercial position. This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible (Adebusuyi, 2008). Such actions can hardly be classified as theft or even malicious damage.

Categories of Cyber-Crime

Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hacker's crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders (Okonigene and Adekanle, 2009). Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring in experienced cyber-criminal large cash resulting from very little effort.

Computer Virus: Viruses and worm are a major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples. Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained (Okonigene and Adekanle, 2009).

Spamming: Involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regard to bandwidth consumption but also to the amount of time spent downloading/eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the email's contents and use of imagery that cannot be detected by spam filters (Oliver, 2010).

Financial Fraud: These are commonly called "Phishing' scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim's bank.

Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from a victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software (Mohsin, 2006). Hackers can also monitor what you do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company (Longe and Chiemeke, 2008).

Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.

Cyber harassment: is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.

Cyber laundering: is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

Website Cloning: One recent trend in cyber-crime is the emergence of fake 'copy-cat' web sites that take advantage of consumers who are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit (Oliver, 2010). The consumers, believing that they are entering credit details in order to purchase goods from the intended company, are instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

Effects of Social Media and Cyber-Crime

The effects of social media and cyber-crime as summarized by Oliver (2010) include;

Financial loss: cyber-criminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals through social media platforms.

Loss of reputation: most companies that have been defrauded or reported to have been faced with cyber-criminal activities complain of clients losing faith in them especially through the use of social media platforms.

Reduced productivity: this is due to awareness and more concentration being focused on preventing cyber-crime and not productivity.

Vulnerability: Vulnerability of their Information and Communication Technology (ICT) systems and networks.

Challenges of Social Media and Cyber-crime

According to Tunji (2012), the rate of e-crime in Nigeria has outgrown the rate of Internet usage in the country. He said Nigeria is the 56th out of 60 countries embracing Internet usage but third in the fraud attempt category. The challenges of social media and cyber-crime as highlighted by Waziri (2009) include;

Domestic and international law enforcement: A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic (Oliver, 2010).

Unemployment: The state of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. Companies are also embarking on mass sack of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions (Olumide and Victor, 2010). Most young youths have no other option than to engage in cyber-crime through the use of social media.

Poverty Rate: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries. Most people out of poverty are forced into engaging in cyber-crime through the use of social media.

Corruption: Nigeria was ranked third among the most corrupt countries in the world. According to Olumide and Victor (2010), until 1999, corruption was seen as a way of life in Nigeria. Corruption in Nigeria has made people to see cyber-crime as a normal thing rather than see it as a criminal act. Social media is now used to defraud people and companies.

Lack of Standards and National Central Control: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse (Olumide and Victor, 2010; Ivwighren, Igben & Ogwezi, 2023).

Lack of Infrastructure: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

Proliferation of Cybercafes: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service, they provide to prospective customers without being guided or monitored. This has given rise to cyber-crime in our modern-day society.

Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

Theoretical Framework

The theory of social media as postulated by Barzilai (2003) posits that social media allow users to meet online via the internet, communicate in social forums like Facebook, Twitter, Instagram, Badoo, BB, and other chat sites, where users generally socialize by sharing news, photo or ideas and thoughts, or respond to issues and other contents with other people. Social media according to Barsh (2013), are technologies that facilitates social interaction, make possible collaboration, and enable deliberation by stakeholders across boundaries, time and space. These technologies include: blogs, wikis, media (audio, photo, video, text) sharing tools, networking platforms, and virtual worlds.

The theory of social media as used by Boyd and Ellison (2007), explains that media which is an umbrella term for various means of communication, has become an integral part of human life around the world. As pointed out by Chalamalla (2012), the World Wide Web is altering human social interaction and the way the brain processes information. Consequently, scholars dive into the potential of internet addiction and the internet's effect on other behavioural changes. Majority of research focus on the true aspects of addition and assess whether internet addiction actually exists. Although research is scanty in assessing whether youths are addicted to social media use, some scholars have done some work on it and various researchers have tested social media addiction with a small sample.

The theory of social media is generally used to describe collaborative media creation and sharing on a fairly large scale but can be extended to include smaller users-generated content networks or micro-communities (i.e. the small media aspect of the current media environment), and things that sometime fall outside SNS such as blogs, podcasts, wilds, game modding (Boyd and Ellison, 2007; Okereka, Orhero & Okolie, 2024). Brett (2015) opined that social media sites in particular had a profound effect by changing the nature of efficiency of communication processes in both business and private life. Brett (2015) defined social networking sites as the set of people or rather other social entities such as organizations connected by a set of socially meaningful relationship. The social networking sites are considered to provide a platform for social relations whereby people share activities, ideas, events and interests. Social media are communicators of the public. Today its role extends not only to giving facts as news, it also analyses and comments on the facts and thus shapes the views of the people. The impact of social media on society today is beyond doubt and debate (Joseph, 2017). The social media has been setting for the nation its social, political economic and even cultural agenda. With the advent of satellite channels its impact is even sharper and deeper. With twenty-four hours news-channels, people cannot remain neutral to and unaffected by what the channels are serving day and night. It is, therefore, of paramount importance that the social media plays an important and ethical role at all levels and in all parts of the country and the world despite its negative effects in promoting cyber-crime.

Empirical Studies

The related empirical studies for this study include the review of studies on social media and cyber-crime among Abraka residents. Studies conducted by Agbanu and Nwabueze (2011) and Ivwighren et al. (2023) describes social media as a variety of new sources of online information that are created, initiated, circulated and used by consumers' intent on educating each other about products, brands, services, personalities and issues. The study carried out by Agbanu and Nwabueze (2011) also analyzed the negative consequences of social networking site especially in promoting cyber-crime. Despite the positive gain, it comes with the negative impact of it. According to Chauhan (2004) in a survey of United Kingdom companies, 233 million hours are lost every month as a result of employees wasting time on social networking sites. Chauhan (2004) in a study of 935 participants in American revealed that 55% of youths used social networking sites in 2006. The main reasons reported for this usage were 'staying in touch with friends' and 'using them to make new friends. However, the study carried out by Ibikunle and Eweniyi (2013) emphasized on the impact of social media on cybercrime, stressing on the negative impact in encouraging criminal activities and computer hacking. The study emphasized the need for the society to create a balance between social media and their daily lives to prevent setbacks.

But the reviewed study carried out by Forsythe (2009) failed to throw more light on the negative influence of social media on cybercrime and internet theft. The present study therefore analyzed both sides of the coin giving the society the opportunity to choose what impact they want the social media to play in their daily lives. Forsythe (2010) in a study reported that users are the core of the social networking sites that without them there would be empty forums, chat rooms and even application. Users are the one who direct and provide dynamics in network. Interaction is another exciting characteristic of social networks whereby connecting to one another and have funs with friends is a priority. Social networks thrive on relationship in a way that more relationship in a network than more profound is the network and stronger it becomes. In a similar study carried out by Schaeffer (2009), social media was related to cyber-crime. He emphasized that the term cyber-crime security is used to "summarize various activities such as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Odumesi and Olayemi (2014) found that cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developing countries as Nigeria. They also observed that cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult. Okonigene and Adekanle (2009) found out in similar study that cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminals large cash resulting from very little effort.

RESEARCH METHODS

This study adopted the survey research method in the collection of meaningful and relevant information on social media and cyber-crime among Abraka residents, and the extent to which social media have been used to perpetuate cybercrimes. The population used for this study is 128,916 people (National Population Commission, 2006) comprised of social media users in Abraka Community especially in areas where most cyber-crimes are being committed on regular basis. This is to truly point out and reflect the extent to which social media has been used to perpetuate cyber-crime. A sample of three hundred (300) respondents comprising of social media users was therefore selected from the given population (128,916) using the systematic sampling technique. The sample of the selected social media users (300) was based on the simple random sampling techniques. About thirty (30) respondents each were selected from seven (7) different locations/zones in Abraka while ninety (90) respondents were selected in Abraka P.O making it a total of three hundred (300) respondents used as the sample size. About 91% of the questionnaires administered comprising of two hundred and seventy-five (275) copies were returned from the respondents after completing them within an interval of one week. The data collected for this study through the administration of questionnaire were analyzed using the inferential and descriptive statistical techniques. These statistical tools were used because they were suitable means of breaking down and analyzing the data that were generated.

Research Results

Research Question 1

To what extent are social media users aware of the use of social media platform to perpetuate cyber-crimes?

Table 1: Extent to which social media users are aware of the use of social media platform to perpetuate cyber crimes

Response	**Frequency**	**Percentage (%)**	**Mean (X)**	**Standard Deviation**
Aware	153	56	91.67	63.07
Not aware	95	34		
Undecided	27	10		
Total	**275**	**100**		

Source: Fieldwork, 2018 **>25.0 Aware** **<25.0 Not aware**

From the table above, research question one analyzed the extent to which social media users are aware of the use of social media platform to perpetuate cyber-crimes. It could be deduced that about 56% of the social media users are aware of the use of social media platform to perpetuate cyber-crimes while 34% are not aware.

The calculated mean value of 91.67 is significantly higher than the mean standard value of 25.0 indicating that social media platforms such as Twitter, Facebook, Whatsapp, and Instagram can be used to perpetuate cyber-crimes. The standard deviation value of 63.07 also showed that there is significant variation to the extent to which social media users are aware of the use of social media platforms to perpetuate cyber-crimes.

Research Question 2

What significant influence do social media have on cyber-crime?

Table 2: Influence of social media on cyber-crime

Response	**Frequency**	**Percentage (%)**	**Mean (X)**	**Standard Deviation**
Agreed	191	70	88.33	89.05
Disagreed	42	15		
Undecided	32	12		
Total	**275**	**100**		

Source: Fieldwork, 2018 **>25.0 Agreed** **<25.0 Disagreed**

From the table above, research question two analyzed the responses of the social media users on the influence of social media on cyber-crime. It could be deduced that 70% of the social media users agreed that social media has significant influence on cyber-crime while 15% disagreed.

The calculated mean value of 88.33 is greater than the mean standard value of 25.0 indicating that social media have significant influence on cyber-crime. The standard deviation value of 63.07 also showed that there is significant variation in the influence of social media on cyber-crime.

Research Question 3

What are the types of cyber-crime associated with social media?

Table 3: Types of cyber-crime associated with social media

Types	Frequency	Percentage (%)	Mean (X)	Standard Deviation
Computer hacking	49	18	39.29	20.28
Cyber theft	67	24		
Financial fraud	54	20		
Internet fraud	44	16		
Cyber harassment	32	12		
None	8	3		
Others	21	8		
Total	**275**	**100**		

Source: Fieldwork, 2018 **>25.0 Agreed** **<25.0 Disagreed**

From the table above, research question three analyzed the various types of cyber-crime associated with social media. It could be deduced that computer hacking (18%), cyber theft (24%), financial fraud (20%), internet fraud (16%) and cyber harassment (12%) are the various types of cyber-crime associated with social media.

The calculated mean value of 39.29 is greater than the mean standard value of 25.0 indicating that the use of social media platforms such as Twitter, Facebook, Whatsapp, and Instagram have contributed to the various types of cyber-crimes. The standard deviation value of 20.28 also showed that there is significant variation in the contribution of social media platforms to cyber-crime.

Research Question 4

What significant effect does social media-aided cyber-crime have on its users?

Table 4: Effect social media-aided cyber-crime on social media users

Effects	Frequency	Percentage (%)	Mean (X)	S.D
It leads to loss of valuable information	53	19	45.83	19.76
It leads to huge loss (finance)	62	23		
It has direct effect on economy and security	60	22		
It leads to total collapse of businesses and reduced productivity since most victims find it difficult to cope after been defrauded	48	17		
No idea	8	3		
Others	44	16		
Total	**275**	**100**		

Source: Fieldwork, 2018 **>25.0 Agreed** **<25.0 Disagreed**

From the table above, research question four analyzed the significant effect social media-aided cyber-crime has on its users. It could be deduced that loss of valuable information (19%), financial loss (23%), economic lost and insecurity (22%), and collapse of businesses and reduced productivity since most victims find it difficult to cope after been defrauded (17%) are the major significant effect social media-aided cyber-crime have on its users. The calculated mean value of 45.83 is greater than the mean standard value of 25.0 indicating that social media-aided cyber-crime have significant effect on its users. The standard deviation value of 19.76 also showed that there is significant variation in the effect of social media-aided cyber-crime on its users.

DISCUSSION

The analysis obtained in research question one showed that social media platforms such as Twitter, Facebook, Whatsapp, and Instagram can be used to perpetuate cyber-crimes since the result shows that 56% of the social media users are aware of the use of social media platforms to perpetuate cyber-crimes while 34% are not aware. These findings conform to Social Media Theory as postulated by Barzilai (2003) and used by Boyd and Ellison (2007) and Barsh (2013). The theory explains that media which is an umbrella term for various means of communication, has become an integral part of human life around the world. These findings also corroborate to that of Baruah (2012) who found that social media platforms such as Whatsapp, Facebook, Twitter, Youtube, Badoo, Instagram and BBM, among others are basically internet social networking sites that connect people together for a variety of purpose, ranging from friendship, chatting, courtship, commerce, education to mass communication and can be used to perpetuate cyber-crime.

The analysis obtained in research question two revealed that social media have significant influence on cyber-crime since 70% of the social media users agreed to this view while 15% disagreed. This is in line with the findings of Abdulahi, Samadi, and Gharleghi (2014) who looked into the negative impact of social media and found that lack of control of the social media can create room for vices, such as falsification, incredibility, unprofessionalism, falsehood, sedition, blackmail, pornography, invasion of privacy, and other unacceptable practices such as increased rate of cyber-crime. These findings conform to Use and Gratification Theory as used by Dennis (1994) and Okenwa (2002) which presupposes that members of the public will actively select and use specific forms of media content to fulfill their interest and motives. This is also in line with the findings of Karen and Pinchot (2012) who looked into the negative side of social media platforms and found out that social media has made it easier for cyber criminals to target victims through the gathering of their relevant information from the internet.

The analysis obtained in research question three revealed that the use of social media platforms such as Twitter, Facebook, Whatsapp, and Instagram have contributed to the various types of cyber-crimes since computer hacking (18%), cyber theft (24%), financial fraud (20%), internet fraud (16%) and cyber harassment (12%) constitute the various types of cyber-crime associated with social media. Thes e findings conform with Social Media Theory as used by Roland (2015) who believe that social media and social change can have implications on the past, present and future. This is in line with the findings of Long and Chiemeke (2008), Augustine (2010), Anderson (2012), and Laura (2015), who found out that social media and cyber-crime are causing near total collapse of most cities in Nigeria particularly Lagos, Warri, Port-Harcourt, Calabar and Abuja, with over 90% of criminal activities coming from the social media platforms Twitter, Facebook, Whatsapp, Youtube, Badoo, BBM, and Instagram. The reason for this trend is that it is easier to perpetuate cyber-crime through social media platform.

The analysis obtained in research question four showed that social media-aided cyber-crime have significant effect on its users since loss of valuable information (19%), financial loss (23%), economic lost and insecurity (22%), and collapse of businesses and reduced productivity since most victims find it difficult to cope after been defrauded (17%) constitute the major significant effect social media-aided cyber-crime have on its users. This finding conforms to the Technical Determinism Theory as postulated by Baran (2004) and used by Chandler (2015) in explaining the fact that social media and technology is neutral, its significance lies in the way people use it. This is in line with the findings of Augustine (2010), who found out that cyber-crimes entail all social media triggered-aided crimes, and other crimes committed with the aid of a computer network. In it are embedded a lot of alarming criminal activities, which have ruined a lot of individuals, organisations and even companies. This finding also conforms with that of Joseph (2017), who found that social media, with its positive impact, have brought serious threat to the society with the advent of cyber-crime.

CONCLUSION

Based on the result obtained from the research findings the study concluded that social media platforms such as Twitter, Facebook, Whatsapp, and Instagram can be used to perpetuate cyber-crimes. Social media have significant influence on cyber-crime and that social media has made it easier for cyber criminals to target victims through the gathering of their relevant information from the internet. The study also conducted that the use of social media platforms such as Twitter, Facebook, Whatsapp, and Instagram have contributed to the various types of cyber-crimes and that it is easier to perpetuate cyber-crime through social media platforms. Finally, the study concluded that social media-aided cyber-crime have significant effect on its users and that social media, with its positive impact, have brought serious threat to the society with the advent of cyber-crime. Based on the findings of this work, the following recommendations are made:

1. One of the best ways to prevent cyber-crime is to have the knowledge of security consciousness, been alert and having security awareness.
2. There should be stringent policies and sanctioning of offenders who engage in cyber-crime and internet fraud.
3. There is need for continuous update/broadcast of cyber-crime events. This will keep the masses and social media users abreast of cyber-crime cases in the country.
4. The knowledge about computer hacking should be limited to professionals. This can best be done through restriction of relevant information to other internet users.
5. Vital information should not be disclosed on the internet for the general public to have access to anytime. There should be strict restriction of vital information among individuals, organizations and companies. This can best be done by avoiding multiple-public device usage to link information on the internet.

6. The use of password codes among social media users should be encouraged. This will help restrict relevant information on the internet from other users so as to be on the safer side.

References

Abdulahi, A. Samadi, E. and Gharleghi, I. (2014). Negative impact of social media. *International Journal of Mass Communication*, Vol. 3(6), 45-49.

Abouharb, R. and Cingranelli, D. (2007). *"Human Rights and Structural Adjustment"*. New York: Cambridge University Press.

Adebusuyi, A. (2008). The Internet and Emergence of Yahoo boys sub-Culture in Nigeria. *International Journal of Cyber-Criminology*, Vol. 2(2), pp. 368-381.

Amedie, S. (2015). Anatomy of communication. Abeokuta: *Julian Publishers*.

Anderson, J. and Bernoff, J. (2010). A global update of social technographics. *Forrester Research Report*. September 28, pp. 12-18.

Anderson, R. (2012): *Measuring the cost of cybercrime*, 11th Information and Communication Technology (ICT) Workshop on the Economics of Information Security (June 2012).

Augustine, C. O. (2010): *Cybercrime & Cert: Issues & Probable Policies for Nigeria*, DBI Presentation, Nov 1-2.

Baran, S. J. (2004). Introduction to mass communication: media literacy and Culture: (3rd edition). New York: McGraw hill companies.

Barsh, R. (2013). “Measuring Human Rights: Problems of Methodology and Purpose.” Human Rights Quarterly, 15: 87-121

Baruah, R. L. (2012). Communicative, Connective and Interactive Potency of Social Media. *In covenant Journal of Communication (CJOC)*, Vol. 1, Pp. 43-55.

Barzilai, G. (2003), Communities and Law: Politics and Cultures of Legal Identities. The University of Michigan Press.

Boyd, D. and Ellison, B. (2007). Social network sites: Definition, history and scholarship”. *Journal of Computer-Mediated Communication*, Vol. 5, pp. 210-230.

Brett, S. (2015). What can social media platforms do for human rights?

Chalamalla, V. (2012). The Role of Media and the Protection of Human Rights: A Historical Perspectives, *Human Rights Protection*, Vol. 24, pp. 764-766.

Chandler, D (2015). Technological or Media Determinism. Retrieved 18 September 2015 from <http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html>

Chauhan, O. P. (2004). Human Rights: Promotion and Protection. Anmol Publications PVT. LTD.

Ellison, B., Esra, A.S. and Melissa, T. (2007). Social Media Platforms and Cyber-crime. Journal of Human Rights, Vol. 2(4), pp, 24-39.

Esra, A. S., and Melissa, T. (2017). It’s About Human Rights: Social Media Platforms Must Safeguard Citizen-Generated Content. *Journal of Human Rights*, Vol. 2(1), pp. 10-14.

Forsythe, F. P. (2010). Human Rights in International Relations. Cambridge: Cambridge University Press. International Progress Organization.

Ibikunle F. and Eweniyi, O. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education*, Vol. 1(1), pp. 19-28.

Ivwighren, H. E., Ogwezi, J. O. & Igben, H. G.O. (2023) Relationship Between Digital Advertising and Consumer Purchasing Behaviour in Delta State, Nigeria. European Journal of Business and Innovation Research, 11 (7). pp. 87-102. ISSN 2053-4019(Print), 2053-4027

Ivwighren, H.E., Igben, G. O. & Ogwezi, Joyce. (2023). Influence of Digital Advertising on Consumers Buying Behaviour in Delta State. British Journal of Marketing Studies. Vol. 11. 40-58. 10.37745/bjms.2013/vol11n14058.

Joseph, S. (2017). Negative effects of cyber crime. *Journal of Communication*; Vol. 1(2), pp. 4-5

Karen, S. and Pinchot, C. (2012). Negative impact of Facebook. *Interdisciplinary Journal of Research Business*, Vol. 1(3), pp. 11-19.

Kaye, D. (2017). Freedom of expression and opinion. United Nations rapporteur, New York.

Laura, A. (2015) "*Cyber Crime and National Security: The Role of the Penal and Procedural Law*", Research Fellow, Nigerian Institute of Advanced Legal Studies.

Liang, C. S. (2012) "Terrorism, Organised Crime and Cyber Security." *International Journal of Security Management*; Vol. 1(2), pp. 73-81.

Longe, O. B, and Chiemeke, S. (2008): Cyber Crime and Criminality In Nigeria-What Roles Are Internet Access Points In Playing*?, European Journal Of Social Sciences*, Vol. 6(4), pp. 1-14.

Mohsin, A. (2006). *Cyber Crimes and Solutions*. Evans Book Publishers, Ibadan, pp. 13-18.

Moses, O., and Roseline, O. (2012). Cyber Capacity without Cyber Security: A Case Study Of Nigeria's National Policy For Information Technology (NPFIT)*, The Journal of Philosophy, Science & Law*, Vol. 12, pp. 21-28.

Murphie, A. and Potts, J. (2013). "1". Culture and Technology. London: Palgrave. p. 21

Nojeim, G. T. (2009), *Cyber security: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace.* Statement before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security.

Odumesi, J. and Olayemi, E. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria-Learning Department, Civil Defence Academy, Abuja, FCT Nigeria. *International Journal of Sociology and Anthropology*, Vol. 6(3), pp. 116-125.

Okenwa, G. (2002), Teaching in mass communication: a multi-dimensional Approach. Enugu: *New Heaven Books.*

Okereka, O. P., Orhero, A. E., & Okolie, U. C. (2024). Digital media and data collection in social and management sciences research in Nigeria. *Ianna Journal of Interdisciplinary Studies,* 6(1), 76 – 89. https://doi: 10.5281/zenodo.10865964

Okolie, U. C., Udom, I. D., Okoedion, E. G. and Fasingha, W. (2023). National information communication technology policy and teaching quality in Nigerian universities. *Indonesian Journal of Digital Business*, 3(1), 8 – 35.

Okonigene, R.E. and Adekanle, B. (2009): *Cybercrime in Nigeria, Business Intelligence Journal*, Vol. 1(2), pp. 1-9.

Okunna, S. C. (1999). Introduction to mass communication. Enugu*: New Generation Books.*

Oliver, E. O. (2010): *Being Lecture Delivered at DBI/George Mason University Conference on Cyber Security holding,* Department of Information Management Technology Federal University of Technology, Owerri, 1-2.

Olumide, O. O. and Victor, F. B. (2010): E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology*, Vol. 11(1), pp. 10-20.

Schaeffer, B. S. (2009): *Cyber Crime and Cyber Security*. A White Paper For Franchisors, Licensors, and Others.

Waziri, J. R. (2009). The dynamic of mass communication: media in the digital Age (7th edition). *New York: McGraw Hill*.

Yar, E. (2005). Mass communication: an introduction: (3' edition). New Jersey: Prentice Hall Incorporation.