International Journal of Social Sciences and Humanities Invention 10(05): 7839-7852, 2023
DOI: 10.18535/ijsshi/v10i05.02
ISSN: 2349-2031
https://valleyinternational.net/index.php/theijsshi

Perceptions of undergraduates towards cybercrimes at the University of Nigeria, Nsukka

Ijeoma B. Uche[1] & Okala A. Uche[1]

[1]Department of Social work, University of Nigeria, Nsukka

Abstract
Cybercrimes are violations committed against a person or a group of persons to hurt innocent people and gain financial advantage. Several people, especially young ones, are seduced by cybercrimes for a variety of reasons. The undergraduate students of the University of Nigeria, Nsukka attitudes regarding cybercrime are the subject of this study. During focus group discussions, data from 54 UNN undergraduates were gathered using an explorative research design. They were chosen at random from the institution's six departments. Themes were used to analyze the data. Study findings showed that every participant was aware of cybercrimes. The main effects of cybercrime on undergraduates were disruptions to students' academic activity, which in turn caused trauma and depression. In line with the study, the government should make sure that the existing cybercrime laws are fully implemented. Moreover, experts like social workers could be able to rehabilitate repented cybercrime perpetrators through education and counseling.

Keywords: Cybercrime, Perception, Perception of undergraduates, Undergraduates, University of Nigeria, Nsukka.

Introduction

Criminal acts including theft, fraud, forgery, insult, and other wrongdoing committed online are referred to as cybercrimes. Cybercrime is viewed as a complicated crime that occurs in limitless cyberspace and is made worse by the growing participation of organized crime. Cybercrime has an international reach since both its perpetrators and its victims are frequently dispersed geographically. Cybercrime has become more prevalent and straightforward to commit. It is more difficult for law enforcement officials to halt the trend, because of the improvement in technology. Since they are less equipped to defend themselves from cyberattacks, developing nations in particular have greater victimization rates. Protecting people from cybercrime must be a top concern for all countries (United Nations Office on Drugs Commission [UNODC], 2005).

Reep-van den Bergh and Junger (2018) conducted a systematic review and found that the yearly criminal incidence rates in Europe varied from 1 to 3% for online shopping fraud and 1 to 2% for online banking/payment fraud. Some forms of fraud affect less than 1% of the population, while online abuse, such as stalking and threats, affects no more than 3% of the population. Hacking affects 1-6% of people. Nigerian students at higher institutions are active in cybercrime, according to Odo and Odo (2015). Gender and type of institution have an impact on engagement. Ige (2018) found that students' perceptions of cybercrime produced high mean scores in a similar vein. Cybercrime is the term used to describe crimes performed online utilizing computers as either a tool or a target. Any criminal operations carried out by one or more individuals referred to as scammers, hackers, or online fraudsters are included (Lexis, 2013). In recent years, cybercrime has gotten increased attention. The possibility of criminal exploitation has grown as more daily activities such as banking, commerce, communication, and entertainment have moved online. The openness and size of the internet are exploited by criminals to scam people in a sophisticated underground economy (Moore, Clayton, & Anderson, 2009).

According to UNODC (2005), cybercrime is a developing subset of transnational crime. It is common knowledge that information and communication technology, or ICT, sometimes known as IT, satisfies a range of user demands, including those related to education, entertainment, communications, and business.

But despite these advantages, technology has also given rise to a brand-new wave of illegal activity known as cybercrime (Mshana, 2015). According to Saban, McGivern, and Saykiewicz (2002), these criminal actions include any unlawful conduct made possible by a computer, regardless of whether the computer is the target of the crime, the tool used to perform the crime or the source of evidence required to prove the crime. Cybercrimes are defined as crimes performed in an online or electronic setting. Although the fast advancement of digital technology and computer networking has many positive implications for human existence, it has also had negative repercussions that have given rise to a variety of online issues known as cybercrime (Asokhia, 2010; Mensch & Wilkie, 2011).

Cybercrime is a global phenomenon that occurs everywhere. According to Calum (2014), the cyber threat in the United Kingdom (UK) continues to be a tier-one national security danger. One of the three main dangers to UK cyber security is the illicit usage of the internet. There is greater potential for people to use the internet for illegal purposes as internet usage and accessibility rise and more and more public and private assets are held online rather than physically. Almost 1.8 billion people utilize the internet worldwide (Javelin Strategy and Research, 2009). Hackers now have more targets to attack as well as new, more profitable possibilities as internet use and technology have advanced (Lance, 2009). Longe, Ngwa, Wada, Mbarika, and Kvasny (2009) reported that Ghana, Nigeria, and Cameroon are three of the top ten countries in the world for producing cybercrime. In Ghana, cybercrime is a relatively recent phenomenon (Warner, 2011).

According to the Centre for Strategic and International Studies [CSIS] (2014), cybercrime causes the global economy to lose 445 billion dollars annually. Statistics on cybercrime and a rising number of studies show that young people do not always act morally in online interactions, thus there is a risk for any internet user to become a victim (McQuade, 2009). In Nigeria, cybercrime has been a widespread occurrence, particularly among undergraduate students.

Computers and networks are used in cybercrime, often known as computer-related crime. A recession or economic meltdown might entice university freshmen to commit cybercrime. Some cyber criminals use it as a great social tool for self-improvement, entertainment, learning, and the pursuit of financial gain (Igba, Igba, Nwambam, Nnamani, Egbe & Ogbodo, 2018).

According to Bidgoli, Knijnenburg, and Grossklags (2016), undergraduate students are more susceptible to cybercrimes because of their increased technological involvement and growing financial and social independence. It was also discovered that for knowledge about cybercrime and cyber security, this group largely relies on the media and individuals they directly know. Most students did not have the necessary information on how to report cybercrime formally. The grouping of undergraduates who are largely involved in cyber fraud based on their age, sex, caste, socioeconomic status, and a plethora of other variables frequently serves as the basis for affiliation and proximity in the fraud world (Bidgoli, Knijnenburg & Grossklags, 2016).

The widespread poverty and high levels of corruption are the key factors driving cybercrime among university undergraduates. Akpan (2016) reported that since the tools for hacking have become so accessible, students are now really seeking money to become the greatest hackers or to start profitable businesses. Most Nigerian undergraduates are reportedly living in poverty (below $1, or 360 naira a day). To pave the way for tomorrow, more than 5 million Nigerian university undergraduates turn to cybercrime. They have no idea what they will do when they graduate from the institution (Igba, Igba, Nwambam, Aja, Egbe & Ogbodo, 2018).

Every facet of human endeavors is crucial to the social work profession, particularly when there is a risk of dysfunction and unethical behavior. According to the International Federation Association of Social Work [IFSW] (2014), social work is a field of study that promotes social growth, stability in society, and the emancipation of those who are weak and oppressed. Also, it supports social justice, human rights, and group accountability. The fundamental premise of the social work profession is respect for people from all backgrounds. This suggests that among other functions, the social work profession serves the purpose of providing individuals, even students, with an education that would eventually set them free from cybercrime. Social workers are tasked with addressing issues of social justice and human rights concerns on behalf of the public. To carry out this mandate, social workers promote the standardization and coordination of cyber security awareness and education programs at all levels of education, ensure that there are capacity-

building programs for cybercrime law enforcement agencies, and facilitate the review of criminal laws and the enactment of cyber laws to address cybercrime (Odumesi, 2014).

Every government in the world owes its population a fundamental responsibility to safeguard and ensure the security of their lives, property, and overall quality of life (United Nations, 2015). The effects of cybercrime on national growth, however, are tearing deeply into the fabric of the world. To achieve sustainable development as envisioned by the United Nations development agenda in 2015, it is crucial to address them.

The intentional emergence of fresh waves of crime has damaged the academic development of undergraduates through the internet. Also, it has evolved into a setting where the most advantageous and secure offense flourishes. Cybercrime has made an unexpected and bizarre appearance that is currently part of our life. As time goes on, we see an increasing number of concerning cybercrimes, with each new instance being more frightening than the last (Okeshola & Adetola, 2013). It is against this backdrop that this article investigates how undergraduates at the University of Nigeria, Nsukka [UNN] perceive cybercrime. The following research questions were addressed in the paper: What are the perceptions of cybercrime?

1. What are the perceived causes of cybercrime?
2. What are the perceived effects of cybercrime?

Answers to these research questions might improve social work practices and the creation of government policies concerning the issues of cybercrime among undergraduates. The paper follows through a detailed review of some relevant literature, a thorough description of the theory, the methodology used, field results, a discussion of the findings, a conclusion, and recommendations that will reduce undergraduates' involvement in cybercrimes.

Literature review

The concept of cybercrime

Cybercrime is a prefix used to identify concepts that are a part of the computer and information era, and crime may be defined as any conduct that violates the law, often carried out by people with criminal intent. Cybercrimes are defined as crimes committed against individuals or groups of individuals with the intent to dishonour the victim's reputation or to directly or indirectly harm the victim's physical or mental health using contemporary telecommunication networks like the Internet (Chat rooms, emails, notice boards, and groups), mobile phones, and other technologies (Halder & Jaishankar, 2011). According to Završnik (2009), the idea of cybercrime itself is still quite nebulous. Cybercrime is a widespread occurrence throughout the world. The term "cyber crime" refers to a series of actions taken by individuals who disrupt networks, steal sensitive information, documents, and bank account information from others, and then move the money to their accounts. The relevance of cybercrime, particularly over the Internet, has increased as computers have become essential for business, entertainment, and government (Goni, Ali, Showrov, Alam & Shameem, 2022). It is a crime to use ICT to conduct traditional crimes as well as crimes that risk ICT's information and network security (also known as computer integrity crimes or cybercrime in a restricted sense) (computer-related crime).

Classification of cybercrime

Vadza (2011) noted that Cybercrime can be classified into two namely:

i. Usage of computer as a target: This means using a computer to attack other computers, for example, Hacking, Virus/Worm attacks and Denial of Service [DOS attack] among others.
ii. Usage of a computer as a weapon: This implies using a computer to commit real-world crimes. e.g. Cyber terrorism, Intellectual Property [IP] infringement, Credit card fraud, Electronic Fund Transfer [EFT] fraud and Pornography among others.

Jahankhani, Al-Nemrat and Hosseinian-Far (2014) further classified cybercrimes into:

- **Pishing**: This is the act of attempting to trick customers into disclosing their personal security information; their credit card numbers, bank account details, or other sensitive information by masquerading as trustworthy businesses in an e-mail. Recipients may be asked to update, validate or confirm their account information.
- **Spam**: Spam mail is the distribution of bulk e-mails that advertise products, services, or investment schemes that may be fraudulent. The purpose of spam mail is to trick or confuse customers into

believing that they are going to receive a genuine product or service, usually at a reduced price. However, the spammer asks for money or sensitive security information like credit card numbers or other personal information before the deal occurs. After disclosing their security information the customer will never hear from the spammer.

- **Hacking**: This is unauthorized access and subsequent use of other people's computer systems (Yar, 2005).
- **Cyber harassment or bullying**: Cyber harassment or bullying is the use of electronic information and communication devices such as e-mail, instant messaging, text messages, blogs, mobile phones, pagers, instant messages and defamatory websites to bully or otherwise harass an individual or group through personal attacks or other means (Early, 2010).
- **Identity theft**: This refers to the act of obtaining sensitive information about another person without his or her knowledge, and using this information to commit theft or fraud (Javelin Strategy and Research, 2009).
- **Plastic card fraud:** It is the unauthorized use of plastic or credit cards, or the theft of a plastic card number to obtain money or property.
- **Internet auction fraud**: Internet auction fraud is when items bought are fake or stolen goods. Sometimes seller advertises nonexistent items for sale which means goods are paid for but never arrive. Fraudsters often use money transfer services as it is easier for them to receive money without revealing their true identity.
- **Malware:** Malware refers to viruses, Trojans, worms and other software that gets into your computer without your knowledge. In some cases, a piece of malware will pretend to be a legitimate piece of software but when it is downloaded, it infects the computer system and destroys valuable information. Trojan horse is also a technique for creating an automated form of computer abuse called the Salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool.
- **Cyberstalking:** Cyberstalking is essentially using the internet to repeatedly harass another person. This harassment could be sexual or have other motivations including anger.
- **Logic Bombs**: A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display gotcha (an authentication method) on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work like viruses (Olusola, Ogunlere, Ayinde & Adekunle, 2013).
- **Password sniffing:** Password sniffers can monitor all traffic in areas of the network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers.

Undergraduates and cybercrime

The world has become a global village. The global infrastructure of information makes it possible for organizations, groups and individuals to have enough and unlimited access to carry out their activities. Nevertheless, it has also led to an increase in cybercriminals as the nature, type, mode, and dynamical sophistication of such attacks are seriously increasing. Nigeria is now ranked 3rd in the world cybercrime (Suleiman, 2019). Information communication technology has disorganized African cultures, patterns of socialization and social institution, particularly concerning telecommunication and the internet. Internet fraud has permeated Nigerian society with undergraduates at the forefront of cybercrime, as the advent of yahoo-boys in tertiary institutions has introduced another dimension of undergraduates' involvement in cybercrime, hence, many undergraduates in Nigeria universities have embraced internet fraud as a way of life; many of them have become rich while others have been caught by the law (Tade & Aliyu, 2011). Out of curiosity to have fun, some skilled undergraduates might fall into the wrong company and may start doing what they think is harmless or simply mischievous, indulge in hacking or using other people's internet profiles and try to do activities that might put them at risk on violating laws (Arasi & Praneetha, 2016). According to the chairman of Nigeria's Economic and Financial Crimes Commission [EFCC], Ibrahim Lamborde, more than 288 persons have been convicted over various internet crimes while 234 are still being persecuted in courts across the country (EFCC, 2012).

The fear of unemployment has been identified as a push factor for undergraduates' involvement in internet fraud. Poverty has risen phenomenally to 40.1% (National Bureau of Statistics, 2018). The involvement of undergraduates in cybercrime may be a creative innovation linked to survival to cope with economic insolvency. University undergraduates are lured into cybercrime as a result of economic meltdown or recession. Undergraduates who go into cybercrime do so as a socio phenomenal which acts as tool for personal development, fun, knowledge and the quest for money making (Igba, Igba, Nwabam, Nnamani, Egbe, & Ogbodo, 2018). Undergraduates might indulge in illegal activities like downloading illegal software, gaining access to pirated files, and hacking and cracking other internet users' computers or even company systems to spread viruses. According to Sargin (2012), it is prominent that most undergraduates in universities are addicted to the internet and fall prey to cybercrime activities as there is significant relationship between internet addiction and cybercrime engagement because an increase in internet addiction and cybercrime engagement will affect the performance and participation of undergraduate students.

Theoretical framework

Many theories of cybercrime abound. However, we are concerned with the perception of cybercrimes among undergraduates. In line with this, we consider the Routine Activity Theory (RAT) as appropriate for the study. Routine Activity Theory (RAT) was first formulated by Cohen and Felson (1979). The focus of Routine Activity Theory is the study of crime as an event, highlighting its relation to space and time, emphasizing its ecological nature and implication. According to RAT, three factors or elements are required for a crime to be present. These elements include: the criminal must be motivated to commit a crime, a suitable target and the absence of a capable guardian who can prevent the crime from happening. These three elements must converge in time and space for a crime to occur. Cohen and Felson (1979) posit that the routine of activities people partake in day and night makes some individuals more susceptible to being viewed as suitable targets by a rationally calculating offender. Routine activities theory relates the pattern of offending to the everyday pattern of social interaction. Crime is therefore normal and is dependent on available opportunities to offend. The presence of a capable guardian is also held to deter individuals from offending. The essential aspect of this theory is the interaction of motivation, opportunity and targets. In this way, the presence of a guardian will deter most offenders, rendering the attractive targets off-limits. Therefore, the presence of opportunity coupled with a lack of guardianship increases criminal motivations and the likelihood of an offence taking place.

Relating this theory to the subject of the study, lack of parental control and motivations from peers (Holt, 2011) are some of the reasons why undergraduates indulge in cybercrime. According to RAT, the absence of a capable guardian is one of the factors that give room for indulgence in crime, where there is no parental control or a capable guardian, youth tend to learn from and influence one another. To this end, motivation and the availability of the internet could lead undergraduates to commit cybercrime. The theory predicts that crime occurs when a motivated offender comes in contact with a suitable target in the absence of a capable guardian that could potentially prevent the offender from committing the crime.

Given that various forms of cybercrime has been acknowledged as some of the biggest threat to individuals and businesses, criminologists have attempted to understand the nature of cybercrime, the characteristics of cybercriminals, and to enhance cybercrime control and prevention. The Routine activity theory was adopted because it proffers an explanation for contemporary cybercrime and virtual criminality primarily in Western countries (Leukfeldt & Yar, 2016).

Cybercrime is usually thought and executed by cybercriminals and does not just occur as cybercriminals go through the process of creating fake accounts to commit fraud or hacking into a person's data, to commit a crime; this is with the first element of routine activity theory which states the presence of a motivated criminal offender with criminal intentions, and the ability to act on this inclination. According to Routine activity theory, cybercriminals commit criminal acts targeted towards unsuspecting persons, who might be careless about their cyber security as a person can hack into another person's account or who might be vulnerable. Most undergraduates reside in the institution without parental guidance and society at large applauds the end and not the means which is a driving force as criminals are being more recognised in the church, family and society; there exists a value distortion and a culture that supports criminality as can be seen in politics for instance, where money is stolen and the politician is being protected; a culture of this nature will not be away from crime. In a bid to keep up with peers and because honest labours are least

recognised, it disposes undergraduates to criminal acts as values are changed. These are propellers predisposing undergraduates to indulge in cybercrimes.

Hsieh and Wang (2018) used RAT in studying a Taiwanese case of an ATM hacking spree. Lhayea (2016) also applied Routine Activity Theory in his study of residential armed robbery in Ghana. Despite the strengths of the theory, there are some weaknesses. Wilcox, Land and Hunt (2003) argued that RAT fails to properly address the role of criminal opportunity contexts – the circumstances in which motivated offenders and suitable targets converge in the absence of capable guardians. Brunet (2002) depicts the weaknesses of RAT on the issue of crime displacement and proper conceptualization of the theory as a micro or macro approach to crime.

Methodology

The study adopted an explorative design that relied on qualitative data research methods. There are 10 faculties at the University of Nigeria Nsukka [UNN]. Multi-stage and simple random sampling techniques were considered appropriate for the study because they enabled the researchers to group the population in stages and finally select the required respondents (Sedgwick, 2015). The first stage was to group the University into faculties. The second stage was to group the faculties into departments. Moreover, the third stage was to group the department into levels of study. A total of six faculties were selected for the study through simple random sampling. They include Faculties of Arts, Biological Sciences, Education, Engineering, the Social Sciences and Vocational Technical Education [VTE]. Also, a total of six departments were randomly selected from the faculties. The selected departments were Mass Communication (in the Faculty of Arts), Biochemistry (in the Faculty of Biological Sciences), Science Education (in the Faculty of Education), Mechanical Engineering (in the Faculty of Engineering), Psychology (in the Faculty of Social Sciences) and Business Education (in the Faculty of Vocational Technical Education). The process was repeated in selecting the participants for the study. Undergraduates in their 300 and 400 levels were selected for the study. This group of students has stayed for more than two years in the university and has also adapted to the system.

The qualitative method of data collection was adopted in the study. The instrument used in generating data was Focus Group Discussions (FGDs). The FGD guide contained unstructured questions which allowed researchers to probe for further responses from the respondents. Six FGD sessions were conducted in the six selected departments. Three FGDs for female undergraduates and three FGDs for male undergraduates were conducted. Each FGD session was made up of 9 participants. In all, a total of 54 respondents participated in the study. The discussion sessions were recorded, and one of the researchers jotted down the non-verbal gestures. The collected data were analysed in themes paying particular attention to the research questions raised. The participants gave both oral and written consent to be part of the study.

Findings

The findings are presented in four themes. It commenced with the socio-demographic characteristics of the participants followed by perceived knowledge of cybercrime, perceived causes of cybercrime and the perceived effects of cybercrime.

Demographic characteristics of the respondents

Table 1 below shows that among the respondents, an equal number of male and female respondents 50% respectively participated in the study. The data revealed that the majority of the respondents were between ages 21 - 25 years (53.7%), while the least age bracket falls within 26 – 30 years (14.8%). In terms of marital status, the findings revealed that the majority of the respondents were single (87%), and only 13% were single. Furthermore, an equal percentage (16.7%) of respondents from the selected faculties and departments participated in the study. The undergraduates' levels of study were evenly (50.0%) selected. Finally, the majority of the respondents (63%) were residing within the campus.

Table 1: Percentage distribution of respondents by their socio-demographic characteristics

Demographic data	Frequency	Percentage

Sex		
Male	27	50.0
Female	27	50.0
Total	**54**	**100.0**
Age		
16years – 20 years	17	31.5
21 years – 25 years	29	53.7
26 years – 30 years	8	14.8
Total	**54**	**100.0**
Marital status		
Single	47	87.0
Married	7	13.0
Total	**54**	**100.0**
Faculty/Department		
Arts (Mass Communication)	9	16.7
Biological Sciences (Biochemistry)	9	16.7
Education (Science Education)	9	16.7
Engineering (Mechanical Engineering)	9	16.7
Social Sciences (Psychology)	9	16.7
Vocational Technical Education (Business Education)	9	16.7
Total	**54**	**100.0**
Level of study		
300 level	27	50.0
400 level	27	50.0
Total	**54**	**100.0**
Place of residence		
Within the campus	34	63.0
Off-campus	20	37.0
Total	**54**	**100.0**

Source: Field survey, 2019

Perceived knowledge of cybercrime

The researchers made an effort to gather information on the participants' knowledge of cybercrime. Findings from the study showed that the majority of participants were familiar with cybercrime. Several participants agreed that cybercrime may be defined as any criminal behavior carried out through computers or mobile devices, regardless of disguise. One of the participants said:

> Nowadays students are glued to their laptops and phones doing all manner of things. Sometimes you see them clustering in areas within the campus where they can have access network to indulge in such activities. What am I even saying, *yahoo yahoo* and *yahoo plus* are forms of cybercrime. The majority of Nigerian students are into one form of internet crime or another it is just that some of the perpetrators are not known and they do these things secretly. For me, cybercrime is harassing people through the internet […] (300-level female participant; Mass Communication).

Another reflected:

> Who among the students does not know what cybercrime is all about? It is not new in the society not to talk of undergraduates. Some of these cybercrimes are being committed on daily basis among the youth. You know these things need a high IQ (Intelligence Quotient) so an illiterate cannot engage in such. Most students buy data to watch pornographic pictures and indulge in all manner of ills (400-level male participant; Business Education).

Another asserts:

> It is a misdeed against another using computer. Cybercrime comes in different forms perpetrated among old and young people alike. Even though it is perpetrated among young people, older ones are also

involved directly or indirectly. Using a computer or phone to steal from people could be referred to as cybercrime (300-level female participant, psychology).

Yet another said:

For me, cybercrime is a very great illness caused by one person to another. It is usually done with phones, laptops, and computers. I think it is the fastest means of making money these days. You know everybody wants to make it big in society. Society calls the perpetrators hackers. Hmmm I call them guys that know the "*in thing*" (400-level male participant; Mechanical Engineering).

Perceived causes of cybercrimes

The researchers sought to know participants' views on the causes of cybercrimes. Findings from the study revealed that there are causes that motivate undergraduates towards cybercrimes. The participants enumerated the causes including poverty, power and fame; and unemployment among others. The majority of the respondents view the socio-economic background of the perpetrators as the main cause of cybercrime. This was expressed in the narrative of a 300-level female participant in Biochemistry who commented, "Poverty does nobody any good. If not for money, the idea of trying to defraud people through the internet would not have arisen".

Another opined:

Undergraduates engage in cybercrime to make ends meet. There are responsibilities facing you as a student which must be met. I do not need to talk of buying textbooks, paying school fees and accommodation fees, feeding, buying cloths and of course man ought to do what he ought to do. Feel relax so that he can excel in society. You know, when you arrive, your girlfriend will feel on top of the world when flashed with goody-goodies [smiles] (400-level male participant; Science Education).

Yet another participant made a similar assertion but added that people engage in cybercrime for the fun of it and to show off. She narrated thus:

I came from a very poor background and I know how hard it is for me to meet up to my responsibilities as a student. I have a friend who sometimes helps out financially and he is one of the happening guys on the campus [*Yahoo boy*]. It is difficult to resist the temptation of collecting gifts from such people. He has told me on several occasions to join him in internet stealing but I refused and I am sure with time he may withdraw his assistance. You see sometimes when this type of pressure becomes too much, you have no other alternative than to yield to such pressure (400-level male participant; Biochemistry).

Another revealed:

The poor economic situation of most families to meet their daily responsibilities is on the increase in the country. One only tries to survive by using what you have to get what one want. If engaging in cybercrime can put food on your table, so be it. When you make money, whether from cybercrime or not, you are respected in society (300-level female participant; Mass Communication).

The Participants further revealed that power and fame were among the factors that influence peer pressure toward cybercrime. This view was buttressed by a 400-level female participant from Business Education. She said, "Boys these days want to make it big. The idea of "get rich quick syndrome" is flowing in everybody's vein. This leads them to engage in cyber activities that are illegal". Another male participant added, "popularity is the order of the day and you can only achieve this when you have the money. Making money through the internet is one of the fastest means of making money and this makes popular".

Another participant believed that:

Power and fame go hand in hand. If you look at our traditional societies these days, one will notice that young people are making money by fair or foul means and they are being recognized in society. Some people will tell you that this and that person have made it. They are recognized in our ruling class, churches and even in schools. Some lecturers tend to respect and adore any student who had made it. They tend to look the other way when such a student defaults to the school rules and regulations. Undergraduates quest for money because of the popularity and power it will give them. Some of them are interested in having a post in the Students Union Government and believe that they will buy their fellow students with their money (300-level male participant; Psychology).

Surprisingly, the researchers observed that undergraduates engage in cybercrime activities for fear of unemployment upon graduation.

A participant noted:

There is no work anywhere once one graduates. For that, finding yourself something to do now through internet hard work is no crime at all. I even know some students who engage in cyber just to make money for the incoming Student Union Government [SUG] election (300-level female participant; Mechanical engineering).

She, however, declined further comments on students she knew that engage in cybercrime in the institution when further probe was made by the researchers.

Another participant expressed:

Undergraduates tend to engage in fraudulent activities online and make money for fear of not getting employment when they graduate. Once the money is made, they feel they have secured their future. To this end, they are not bothered about employment or not because with their already made wealth, they are okay or better still buy jobs for themselves. It creates employment (300-level male participant; Biochemistry).

Furthermore, the participants indicated that the influence of peer pressure is the greatest force pushing cyber crime among undergraduates. A participant maintained:

Everybody wants to belong in this present society. If one does not belong, he or she is an outcast. So to follow the trend, you need to imitate what others are doing. Some undergraduates participate in cybercrime simply because their friend told them one or two things to convince them into indulging (400-level male participant; Psychology department).

Another affirmed:

Yes, I have a cousin who once duped his father with a huge amount of money. On interrogation, he stated that he learned how to defraud people from his friends back at school.

According to him, they normally search the internet looking for whom to defraud. Initially, he does not want to indulge in such but pressure was mounted on him by his close friend to learn. Students at times came to school innocent of societal ills [cultism and cyber fraud], only to be brainwashed by their friends and classmates. This is called moving with the trend or you are left out (400-level male student; Mechanical engineering).

It was also discovered that place of residence has much influence on cybercrime. A 300-level female participant revealed that "undergraduates who reside off campus are vulnerable to the influence of peer pressure in committing cybercrimes. It is this class of students that are more likely to be involved in cybercrime."

Views of respondents on the effects of cybercrime

The researchers sought to know the effects of cybercrime. The majority of the participants revealed that it obstructs undergraduates' academic activities and in turn brings about psychological imbalance. The findings also revealed that it could lead to imprisonment and finally death. A participant said:

The psychological effect of peer pressure influence towards cybercrime is the obstruction of academic activities. An undergraduate who is a cyber criminal is always with his laptop or phone looking for a victim. He takes his academics unserious and this affects his results. By the time the results of his academic performance start coming out, he is traumatized and depressed (400-level female participant, Psychology).

Another participant revealed:

All fingers are not equal as the saying goes. Among peers, some are more intelligent than others. Undergraduates who perpetrate the act of cybercrime do not have the same level of IQ, therefore, some of them may excel even though they have little time for their academics, while those of them below average will suffer it (300-level male participant, Mass Communication).

Yet another said:

Peer pressure can be positive or negative but in this case, its influence is negative because depression sets in when you noticed that you wasted your time trying to make it on the internet illegal activities when your mates must have graduated and started a meaningful life (400-level male participant, Mechanical Engineering).

Another revealed:

[nodding her head in disapproval], There is one thing that these perpetrators do not think about. They forgot that if they are caught in the act, not only will they drop from school but will be

prosecuted. Some of them may face mob action if caught and this may lead to death. The effect is always adverse (300-level female participant; Business Education).

Probing further, the researchers were able to find out that perpetrators act on impulse. This was made known by the views of a female undergraduate from Psychology who said, "I have the opportunity to ask my brother who used to be cybercrime perpetrator the motive behind such action. He categorically told me that he acted on impulse. Once the urge comes, he looks for data to go online".

Another affirmed:

Just as a cigarette smoker smokes on impulse, so also do cybercriminals act on impulse. The impulse to defraud is uncontrollable. To be honest with you, I was once a cybercrime perpetrator and I can assure you that it was not easy on me when I finally disengaged from such acts through the help of my sister. I was so much attached to internet fraud that I have to forget about food. The urge can come at any time even at night (400-level male participant, Business Education).

Discussion of findings

The illness of cybercrime has eaten deeply into the fibre of the country. Cybercrime refers to illegal computer use in criminal activity. For instance, according to Okeshola and Adeta (2013), cybercrime is a worldwide problem. There is greater potential for people to use the internet for criminal purposes as internet usage and accessibility rise, leading to the electronic storage of more public and private assets in more countries (Calum, 2014). This study is anchored on the perceptions of undergraduates towards cybercrimes at the University of Nigeria, Nsukka.

The study findings showed that the participants knew that UNN undergraduates are subject to cybercrime. The participants stated that another name for cybercrime is yahoo plus or yahoo yahoo. This is consistent with the findings of Ibrahim (2016), Akanle, Adesina, and Akarah (2016), and Akanle and Shadare (2019), who found that cybercrime in Nigeria is commonly referred to as "yahoo yahoo" because Yahoo is the most widely used platform and email provider for free and easy access in the nation among the less wealthy internet users. The "yahoo boys" are the people who commit cybercrime. The participants also concurred that cyberstalking is the most common kind of cybercrime among university students. Similar results were obtained by Nalaka and Diunugala in their study (2020).

The researchers sought to know what causes cybercrime. The results showed that poor socioeconomic backgrounds contribute to cybercrime. The need to earn money quickly and easily was what motivated many to engage in cybercrime. Igba, Igba, Nwabam, Nnamani, Egbe, and Ogbodo (2018) came to a similar result in a survey of undergraduates at Ebonyi State University. They argued that the "get rich quick syndrome" could be linked to the secondary cause of undergraduate involvement in cybercrime because more than 5 million undergraduates in Nigerian universities have no idea what they will do when they graduate, so they turn to crime to pave the way for the future. Power and fame were also shown to be contributing variables to cybercrime among students. The research also showed that undergraduate students who engage in cybercrime do so to gain popularity and influence in the Students Union Government (SUG). The study of Jegede, Olowookere, and Elegbeleye (2016), who found that there are a variety of variables encouraging youth engagement in fraud, provided more support for this. Peer pressure, expensive marital or adulterous demands on relationships, family breakdown due to role failure, the pervasiveness of corruption, the poor economic environment, and the need to fit in may all work together to strengthen fraud activism. Studies have generally shown that peer pressure is a substantial contributor to youth misbehaviours (Donohew, Hoyle, Clayton, Skinner, Colon, & Rice, 1999; Dorsey, Sherer, & Real, 1999). The prevailing view among these academics is that group identification affects individual behavior, which implies that a person inside the web of social interaction feels affinity for and craves affiliation with the reference group. We found that committing cybercrime had negative repercussions on UNN undergraduates. The results of the study showed that the consequences of cybercrimes include imprisonment and premature death. It also demonstrated how cybercrime has interfered with students' academic pursuits. The psychological impact of this has a depressive effect. This result is consistent with findings made by Barfi, Nyagorme & Nash (2018) who revealed that the psychological effects of cybercrime lead to a slow nation's growth, progress and development.

The study is relevant to social work practice because social workers focus on issues like harmony, relationships, functionality, peaceful coexistence, order, and justice since these things are essential to a

meaningful and valuable life. With programs for education and counseling, social workers may help prevent cybercrime. According to the study's results, undergraduates engage in cybercrime due to their desire for popularity, money, and protection from their peers. Hence, undergraduates need to have a changed value orientation toward the ways to acquire riches. Conferences, workshops, and seminars might be used for this. The Routine Activity Theory as used in the study has three components—a suitable target, a criminal's motive to commit a crime, and the lack of a skilled guardian who can stop the crime from happening—should also be taken into consideration by social workers. To do this, social workers can stop the drive to commit crimes through counseling and education. With this, the second and third elements will be taken care of. The study will also extend the social worker's perspective while providing services for the rehabilitation of criminals who have been found guilty so that they adopt the best source of income when discharged from prison. As technology advances, social workers should continually hone their skills in using technical tools to stop crimes committed online.

Conclusion

There has always been cybercrime. It is now an issue and a cause for concern for the entire country, not just for people or organizations. This research demonstrates how undergraduates perceive cybercrime at UNN. There are perceived causes of cybercrime as buttressed by the students. This includes the quest for wealth, joblessness after receiving a degree, peer pressure, power, and fame. The disruption of undergraduates' academic activity is one of the main negative effects of engagement in cybercrime. Due to the lack of employment opportunities after graduation and the realization that society does not value the method of making money above the end, students are more likely to participate in illegal activity. Social workers as professionals whose services are designed to help individuals, groups and society attain their life goals are encouraged to educate and counsel undergraduates on the need to make their wealth through legal means.

Recommendations

Based on the findings of the study, the following recommendations were made:

- The School administration should inculcate in school curriculum courses on entrepreneurship and business management in institutions where students can harness their skills and gain vast knowledge. However, where they are in existence should be strengthened and taken more seriously. This could help in alleviating the issue of unemployment resulting in cybercrime and also help undergraduates adopt acceptable means of livelihood.
- Professionals such as Social workers should be trained in forensic science to enable them to educate and bring to the awareness of undergraduates the implication of criminal activities. They will also help rehabilitate repented cybercrime perpetrators and facilitate public enlightenment programmes on cyber security.
- Government should make sure that the existing laws against cybercrime perpetrators are fully implemented in Nigeria. These laws will deter undergraduates from involving in cybercrimes.
- Non- governmental organizations (NGOs) should help in providing skill acquisition programmes that students will engage in after graduation.
- There is also a need for religious bodies to inculcate good morals and dissuade youths against cybercrime activities.

Ethical concern: This manuscript has not been published elsewhere or submitted to any other journal.

Conflict of Interest: The authors declare that they have no conflict of interest.

References

1. Akanle, O. & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, characterization and strategies. *International Journal of Cyber Criminology, 13*(2), 343 – 357.

2. Akanle, O., Adesina, J. O. & Akarah, E. P. (2016). Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. *African Journal of Science and Technology Innovation and Development, 8*(2), 213 – 220.
3. Akpan, C. (2016). University students and cybercrime: An indispensable critical review. *Journal of Sociology*, *2*(2), 181 - 186.
4. Arasi, N., & Praneetha, V. (2016). Internet addiction and cybercrime engagement of undergraduate students. *Journal of Educational Research & Extension, 1*(3), 6-14.
5. Asokhia, M. (2010). Enhancing national development and growth through combacting cyber internet fraud: A comparative approach. *Journal of Social Science*, 23, 13-19.
6. Barfi, K., Nyagorme, P. & Nash, Y. (2018). The internet users and cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region. Retrieved from https://www.researchgate.net/publication/323746025_The_Internet_Users_and_Cybercrime_in_Ghana_Evidence_from_Senior_High_School_in_Brong_Ahafo_Region.
7. Bidgoli, M., Knijnenbury, B., & Grossklags, J. (2016).When cybercrime strikes undergraduates. Retrieved from http://hatlabclemsonn.filess.wordpress.
8. Brunet, J. R. (2002). "Discouragement of Crime Through Civil Remedies: An Application of a Reformulated Routine Activities Theory", *Western Criminology Review* 4 (1): 68-79.
9. Calum, J. (2014). *The threat of cybercrime to the UK: RUSI Threat Assessment*. Retrieved from https://rusi.org/sites/default/files/201406bpthethreatofcybercrime_to_the_uk.pdf.
10. Centre for Strategic and International Studies [CSIS] (2014) Net losses: Estimating the global cost of cybercrime. Retrieved from https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime.
11. Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588 – 608.
12. Donohew, R. L., Hoyle, R. H., Clayton, R. R., Skinner, W. F., Colon, S. E. & Rice, R. E. (1999). Sensation seeking and drug use by adolescents and their friends: Models for marijuana and alcohol. Retrieved from https://pubmed.ncbi.nlm.nih.gov/10487731/. DOI: 10.15288/jsa.1999.60.622.
13. Dorsey, A. M., Sherer, C., & Real, K. (1999). The College Tradition of Drink till You Drop": The Relationship between Students Social Networks and Engagement in Risky Behaviours. *Health Communication*, 4, 313-334.
14. Early, J. R., (2010). Cyber-bullying on increase. Retrieved from http://www.tmcnet.com/usubmit/2010/02/07/4609017.htm.
15. Economic and Financial crimes commission [EFCC] (2012*). Court jails undergraduate 20years over internet scam.*Retrieved from http://www.efcc.nigeria.org.
16. Goni, O., Ali, H., Showrov, A., Alam, M. & Shameem, A. (2022). The basic concept of cyber crime. Journal of Technology Innovations and Energy, 1(2). 29 - 39. , https://doi.org/10.5281/zenodo.6499991
17. Halder, D., & Jaishankar, K. (2011): *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA:IGI Global. ISBN 978-1-60960-830-9.
18. Holt, J. T., (2011). Low self-control, Deviant peer association and juvenile cybercrime.*American Journal of Criminal Justice, 12*(3), 209-221.
19. Hsieh, M-L, & Wang, S-Y. K. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology, 12*(1), 333 – 352.
20. Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*,47, 44-57. DOI:http://dx.doi.org/10.1016/j.ijlcj.2016.07.002.
21. Igba, D. Igba, Aja, N., Nnamani, S., Egbe, E., & Ogbodo, J., (2018).Cybercrime among university undergraduates.*International Journal of Applied Engineering Research, 13*(2), 1144 - 1154.
22. Ige, O. A. (2018). Effects of gender and technology influence on learners' attitude to cybercrime prevention in urban learning ecologies: Lessons for Swedish gymnasiums. *International Journal of Cyber Criminology, 12*(1), 151 – 170.
23. International Federation of Social workers (IFSW) (2014). *General meeting and the IASSW General Assembly,* July.

24. Jahankhani, H., Al-Nemrat, A. & Hosseinian-Far, H. (2014).cyber crime classification and characteristics.
25. Javelin Strategy & Research (2009). Identity fraud survey report: Identity fraud on the rise but consumer costs plummet as protections increase. Pleasanton, CA: author. *Report Preview*. Retrieved from http://javelinstrategy.com/research.
26. Jegede, A. E., Olowookere, E. I., & Elegbeleye, A. O. (2016). Youth identity, peer influence and internet crime participation in Nigeria: A Reflection. *Ife Centre for Psychological Studies/Services, 24*(1), 37-47.
27. Lance (2009). Online banking is booming. Cnet News. Retrieved from http://news.cnet.com/8301-1001-3-10265409-92.html.
28. Leukfeldt, E. R., &Yar, M. (2016).Applyingroutine theory to cybercrime: A theoretical and empirical analysis.*Deviant Behaviour, 377* (3), 263-280.
29. Lexis, N. (2013). True cost of fraud study: Merchants struggle against an onslaught of high-cost identity fraud and online fraud. Retrieved from http://www.lexisnexis.com/risk/insights/2013-true-cosst-fraud.aspx.
30. Lhayea, N. N. (2016). Application of routine activity theory to the study of residential armed robbery in Ghana. *Theses and Dissertations*. Paper 1008.
31. Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal use of information and communication technologies in Sub-Saharan Africa: Trends, concerns and perspectives. *Journal of Information Technology Impact, 9*(3), 155-165.
32. McQuade S. (2009). Understanding and managing cybercrime.Baston: Allyn and Bacon press. *International Journal of Cyber Criminology, 3*(1) 492-493
33. Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information Management Science Journal*, *14*: 91-116.
34. Moore, T., Clayton, R. & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives, 23*(3), 3 – 20.
35. Mshana, J. A. (2015). Cybercrime: An empirical study of its impact in the society-A case of study of Tanzania. *Huria: Kournal of the Open University of Tanzania, 19*(1), 72 – 87.
36. Nalaka, S. & Diunuggala, H. (2020). Factors associating with social media related crime victimization: Evidence from the undergraduates at a public University in Sri Lanka. *International Journal of Cyber Criminology, 14*(1), 174 – 184.
37. National Bureau of Statistics (2018). *2017 demographic statistics bulletin*. Abuja: National Bureau of Statistics.
38. Odo, C. R. & Odo, A. I. (2015). The Extent of Involvement in Cybercrime Activities among Students' in Tertiary Institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology: H Information and Technology, 15*(3). Retrieved from https://www.researchgate.net/publication/321624892
DOI: 10.13140/RG.2.2.23567.28328.
39. Odumesi, J. O. (2014). Combating the menace of cybercrime. *International Journal of Computer Science and Mobile Computing, 3*(6), 980 – 991.
40. Okeshola, B. F., & Adeta, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institution in Zaria-Kaduna State, Nigeria. *.American International Journal of Contemporary Research, 3*(9), 98.
41. Reep-van den Bergh, C. M. & Junger, M. (2018). Victims of cybercrime in Europe: A review of victims surveys. *Crime Science*, 7(5), 2 – 15. Retrieved from https://doi.org/10.1186/s40163-018-0079-3.
42. Saban, K. A., McGivern, E., Saykiewicz, J. N. (2002); A critical look at the impact of cybercrime on consumer behaviour: *Journal of Marketing Theory and Practice*, 10(2), 29.
43. Sargin, N. (2012). Internet addiction among adolescents. *Educational Research and Review, 7*(27), 613 – 618.
44. Sedgwick, P. (2015). Multistage sampling. BMJ Statistics Endgames. DOI: 10.1136/bmj.h4155.
45. Suleiman, A. (2019). Cybercrime and the sociological implication in the Nigeria's tertiary education system. *Fudma Journal of Science, 3*(1), 249-257.

46. Tade, O., & Aliyu, I. (2011) social organisation of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology,* 5(2):860-873.
47. United Nations (2015). Sustainable Development Goals. Retrieved from https://sustainabledevelopment.un.org.
48. United Nations Office on Drugs and Crimes [UNODC] (2005). The Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Retrieved from https://www.unodc.org/unodc/en/cybercrime/index.html.
49. University of Nigeria Academic Planning Unit, Nsukka (2018). 2018/2019 Students population.
50. University of Nigeria (2018). History/Overview. Retrieved from http://www.unn.edu.ng/administration/office-of-the-vice chancellor/records-unit/.
51. Vadza, K. (2011). Cyber crime and its categories. *Indian Journal of Applied Research 3*(5), 129 – 133.
52. Warner, J. (2011). Understanding cybercrime in Ghana.*International Journal of Cyber- Criminality, 5*(1), 736-749.
53. Wilcox, P., Land, K. C. & Hunt, S. (2003). *Criminal circumstance: A dynamic multicontextual criminal opportunity theory.* New York: Walter de Gruyter.
54. Yar, M. (2005). The novelty of cybercrime: An assessment in light of Routine Activity Theory. *European Journal of Criminology 2*(4), 407 – 427.
55. Završnik, A. (2009). Cybercrime - *Definitional challenges and criminological particularities.* oai:ojs.journals.muni.cz:article/2506. Retrieved from https://core.ac.uk/display/230601102?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1