INTERNET PENETRATION AND CYBERCRIME ATTACK IN ABIA STATE, NIGERIA

(FUWJSS)
Volume2 Number 2
September, 2023

Ogochukwu Favour Nzeakor
Peace & Conflict Studies Unit, School of General Studies
Michael Okpara University of Agriculture, Umudike.
Abia State, Nigeria

Alu Alfred Ede
Peace & Conflict Studies Unit, School of General Studies
Michael Okpara University of Agriculture, Umudike. Abia State, Nigeria

Chibuike Ndubuisi Nwoke
Department of Sociology & Anthropology
The Faculty of Social Sciences, University of Nigeria, Nsukka, Nigeria

Samuel Kalu Obasi
Social Science Unit, School of General Studies
University of Nigeria, Nsukka, Nigeria
Corresponding author*: chibuike.nwoke@unn.edu.ng*

Abstract

Arguments persist to canvass that a person could be a victim of cybercrime attack if even the person does not have access to the internet. However, prevailing arguments canvassed a correlation between increased internet penetration and increased cybercrime attacks. Thus, this study examines the relationship between internet penetration and cybercrime attacks in Abia State, Nigeria. Data for this study emerged through the administration of questionnaire to 1104 respondents between the ages of 20 years and 70 years in Abia State, Nigeria. The study's results confirmed that smart phone (61%) and computer (33%) were the most common ICT gadgets owned by respondents. Also, on average, respondents who own smart phone and other gadgets tend to experience more cyberattacks (M = 2.53, $S.D$ = 1.63) than those who own only smart phones (M = 2.17, $S.D$ = 1.41), $t(923) = 3.453$, $p < .05$, r = .11. Facebook (24%) and WhatsApp (23%) were the most commonly operated online accounts; followed by email (19%), Instagram (11%), and Internet banking (10.8%). That about 4 in every 5 respondents operated more than one online account. Respondents who operated/owned more than one accounts are more vulnerable to cyber security attacks (M = 2.43) than those operated only one account (M = 2.16) and those who operated no account at all (M = 2. 03), $f(923) = 2.889$, $p = .05$, r = .10. The study

concludes that internet penetration in Abia State is high and this level of internet penetration influences cybercrime attacks in the State.

Keywords: Internet, cybercrime attack, online account, ICT gadgets, social media

Introduction

Crime is relative to time and space. It changes in line with a given epoch and society due to changing social, economic, political and environmental conditions (Siegel, 2010; Ugwuoke, 2010). The current information society, in addition to its huge positive outcomes, introduced a novel crime known as cybercrime. Cybercrime is defined as illicit activities perpetrated on, through or against computer technologies (Mali, 2008; Siegel, 2010; Gercke, 2012; Olusola, Ogunlere & Semiu, 2013; Malby, Mace, Holterhof, Brown, Kascherus & Ignatuschenko, 2013). Though the history of cybercrime attacks could be traced to early 19th Century (1820) when the workers of Joseph-Marie Jacquard sabotaged his loom (a device that allowed the repetition of a series of steps in the weaving of special fabrics) in France; the phenomenon has however consistently and viciously overrun the nations of the world (Mali, 2008, p. 4). For instance, in the 21st Century, highly sophisticated variants of the cybercrime- including cyber terrorism, cyber warfare, cyber laundering, phishing, botnet attacks, email bombing, Business Email Compromise (BEC), etc- have emerged.

What is more, both the methods of perpetrating cybercrime, and its impacts are also dynamic as they are equally vicious. Offenders are now able to automate attack giving rise to both increased number offences and victimization (Mali, 2008; Gercke, 2012). The scope of cybercrime attacks is consistently widening. Of recent, the Internet Crime Complaint Center reported that there were about 465,177 reported incidents that year. This amounts to one successful attack per 1.12 seconds. Meanwhile, this does not account for attempted attacks or those that went unreported especially from non-western jurisdictions like Nigeria. In fact, about 86.2% of surveyed firms were affected by a successful cyberattacks (Internet crime complaint center, 2016). While the scale of cybercrime attacks is on the increase, a number of intellectual and institutional interventions emerged. Some of such interventions include: legal, technical, organizational/institutional, public-private partnership, international cooperation, law enforcement/capacity building, public awareness (Gercke, 2012; Malby et al, 2013).

Other interventions in the areas of criminal innovation of the cyber offenders, the anonymity of the Internet, the contributions of victims of cyber-attacks, difficulties in accessing electronic evidence, others equally

emerged (Warren & Streeter, 2005; Hansen, 2007; Akuta et al, 2011; Boateng et al., 2011; Wada & Odualaja, 2012; Gercke, 2012; Malby et al, 2013; Liebel, 2013; Leukfeldt et al., 2013; Lee & Sanchez, 2018; Nzeakor, Nwoha & Nwoke, 2022; Nzeakor, Nwokeoma, Hassan, Ajah, & Okpa, 2022; Okpa, Ajah, Nzeakor, Eshiotse & Abang, 2022). For instance, Hansen (2007), Boateng et al. (2011), Liebel (2013), and Leukfeldt et al. (2013) are of the consensus that increasing the awareness of cybercrime scourge holds better promise in reducing the cybercrime victimization curve. There is another crop of scholars who predicated the increasing cybercrime attacks on the rapid expansion of computer connectivity, and the astronomical growth of the number of Internet users (Gercke, 2012; Malby et al, 2013, Nzeakor, 2016).

However, in what appears like a departure from the stance of rapid expansion of computer connectivity, and the astronomical growth of the number of Internet users (see Siegel, 2010; Gercke, 2012; Malby et al, 2013, Nzeakor, Nwokeoma & Ezeh, 2020), Wall (2010) posited that ever since the emergence of the graphic user interface that made the Internet user friendly and popular, networked technologies are still becoming further entrenched in each and every aspect of people's lives. He concluded that even if one does not use the Internet facilities, much of his or her personal details are still stored somewhere on a networked computer.

In seemingly support of Wall (2010), Harvey (2005) posited that the information networks seemingly render individuals vulnerable to an array of potentially predatory others who have their targets within instantaneous reach, unconstrained by the normal barriers of physical distance. This therefore implies that in one way or another, the information society has effects on everybody irrespective of his or her Internet connectivity and usage. The implication of this is that usage or otherwise of Internet facilities does not insulate any one from the potential harm and victimization embedded in the information society.

However, it is important to note that the puzzle presented by the two groups of scholars: those who advocate that one could still be a victim of cybercrime attack whether he accesses the Internet or not (see Yar, 2005; Wall, 2010; Siegel, 2010); and those who canvassed a correlation between increased Internet penetration or usage and increased cybercrime attacks (see Gercke, 2012; Malby et al, 2013, Nzeakor, 2016) has not been satisfactorily resolved. This therefore constitutes the focus of this paper. This paper builds on the previous works as well as provides empirical answers to the above puzzle. It contributes to the cyber-criminological literature by empirically examining the relationship between Internet penetration and cybercrime attacks in Abia State, Nigeria.

The work started by presenting the background of cybercrime and Internet penetration, especially relating to the preponderance of cyberattacks and some of the predicting factors, a well as the conflicting positions of authors. It proceeded to the interconnectivity of information society, internet penetration and cybercrime victimization attacks in Nigeria. Some concepts were clarified, and the theoretical framework was reviewed. After which the research method, measures, analysis, results summary, conclusion and recommendations were presented.

Internet Penetration and Cybercrime in Nigeria

The Internet has now become a lynch pin for illicit profits, and other harmful and criminal activities in today's information society (Mali, 2008; Siegel, 2010; Gercke, 2012; Olusola, Ogunlere & Semiu, 2013; Malby, Mace, Holterhof, Brown, Kascherus & Ignatuschenko, 2013; Internet Crime Complaint Centre, 2021; Nwoke, Nzeakor, Nwoha, Ugwu, Uba-Uzoagwa, & Ikenegbu, 2021; Nzeakor, Nwoha & Nwoke, 2022; Nzeakor, Nwokeoma, Hassan, Ajah, & Okpa, 2022; Okpa, Ajah, Nzeakor, Eshiotse & Abang, 2022).

Granted that there have been several mitigating measures targeted at reducing the curve of cybercrime victimization, studies have shown that the menace of cybercrime victimization has continued unabatedly at global, regional, and national levels (Umoru, 2017; Mbachu & Nazeef, 2017; Internet Crime Complaint Centre, 2019). As a result, Internet-enabled crimes and scams have therefore shown no sign of letting up as the 2019 report of the Internet Crime Complaint Center (IC3) indicates (Internet Crime Complaint Centre, 2019). The 2019 Reports shows that the highest number of complaints and the highest dollar losses reported since the Center was established in May, 2000. In fact, IC3 received 467,361 complaints in 2019, an average of nearly 1300 every day, and recorded more than $3.5 billion in losses to individuals and business victims (Internet Crime Complaint Centre, 2019).

Even when, the 2020 Report of Internet Crime Complaint Centre held that the victimization report decreased, in comparison to those of previous years, the dollar loss astronomically increased (Internet Crime Complaint Centre, 2021). From this angle, a number of authors are of the view that every individual is a potential victim of cybercrime attack- whether one accessed the Internet or not (see Hansen, 2007; Jaishankar, 2010, Wall, 2020; Nzeakor et al, 2022).

On the other divide, authors predicated the increasing incidence of cybercrime attacks on rapid expansion of computer connectivity, and the astronomical growth of the Internet usage (Nzeakor, 2016; Nzeakor et al, 2020). For instance, the global smartphone market has grown significantly

over the years. It reached 671 million in 2012; which represents an increase of 42% over 2011 (The Current State of Cyber Crime, 2013; Akuta, et al, 2011). In 2017, the smart phone shipment was more than a billion with multiple billion dollars investments. It has dropped to about 1.2 billion units in 2022 (The Current State of Cyber Crime, 2013; Akuta, et al, 2011; Counterpoint, 2023). What is more, the current world Internet users as of February, 2023 was put at about 5.3 billion, up from 4.9 billion in the previous year. This share represents 66% of global population.

In Nigeria, it was reported that about 154.3 million people use Internet in Nigeria (Internet World Stats, 2023). And this represents a whopping 77% of Nigerian population. There is suspicion that the increasing Internet penetration has a correlation with the increasing incidence of cybercrime victimization experience among the populace but the patten and degree are not fully known. For instance, as the world records exponential increase in smart phone shipment and Internet penetration, it contemporaneously witnesses exponential increase in cybercrime attacks and victimizations. Consequently, the current cybercrime outlook is very terrific where there were about 153 million new malware samples from March 2021 to February 2022 (AV-Test), a nearly 5% increase on the previous year which saw 145.8 million malware attacks.

In 2019, about 93.6% of malware observed was polymorphic, meaning it has the ability to constantly change its code to avoid discovery (Webroot Threat Report, 2020). Almost 50% of business Personal Computers and 53% of consumer PCs that got infected once were re-infected within the same year (Webroot Threat Report, 2021). The Internet Crime Complaint Center's 2020 report found that there were 465,177 reported incidents that year, which gives one successful attack every 1.12 seconds. It is important to point out that this doesn't account for attempted attacks or those that went unreported. About 86.2% of surveyed firms were affected by a successful cyberattacks (Internet crime complaint center, 2016).

Crime: It refers to those conducts that break the law of the land and are subject to official punishment (Haralambos & Holborn, 2008).

Cybercrime: It is also known as ―computer security incidents‖. It refers to illegal activities that are committed using computer or network; either as a tool, a target, or a platform of such activities (Moulton, 2010). It also refers to the composite of computer, or network-related criminal activities including e-fraud, e-paedophiles, e-sexual grooming, etc.

Cybercrime Victims: This refers to those participants who admitted having experienced any of account hacking; compliance to fraudulent request; cash

transfer to online impostor; responding to spam mails; received personal threats from email/text; personal visit to online acquaintance; viral/malware attack on ICT gadgets; criminal solicitation; damaged/stolen ICT gadgets, etc.

Cybercrime Attacks: It could be conceptualized in this study as various physical, social, psychological, and economic loss, fears, shocks, stresses, injuries, pains, traumas, harms, damages, threats, losses, and harassments individuals suffer on, through the Internet or computer technology devices. It is measured in this study by the respondent's admittance of having experienced any of the followings- account hack; compliance to fraudulent request; cash transfer to online impostor; responding to spam mails; received personal threats from email/text; personal visit to online acquaintance; viral/malware attack on ICT gadgets; criminal solicitation; damaged/stolen ICT gadgets, etc. This was captured in item No.15 of the questionnaire.

Internet User(s): This refers to those who have utilized Internet facilities or any of the ICT devices in their communications and interactions. It also refers to any individual whose personal information is possibly stored somewhere on a networked computer. For our present purpose, almost every person, especially an adult, is an Internet user.

Information Society: It refers to a type of social system, or society structured in tandem with information and communication technology.

Internet Penetration: This refers to the utilization of Internet facilities or any of the ICT devices in communications and interactions. It is operationalized in this study as the number of ICT gadget or online account ownership.

Internet User(s): This refers to those who have utilized Internet facilities or any of the ICT devices in their communications and interactions. It also refers to any individual whose personal information is possibly stored somewhere on a networked computer. For our present purpose, almost every person, especially an adult, is an Internet user.

Irregular Internet Users: This refers to those participants who do not access or use the Internet daily.

Regular Internet Users: This refers to those respondents who access or use the Internet on daily basis.

Theoretical Framework: Deviant Place Theory

Among the proponents of deviant place theory are Wright and Rossi (1983), and Kleck and Gertz (1998). According to the theory, the greater their exposure to dangerous places, the more likely people will become victims of crime and violence. Victims do not encourage crime but are victim prone because they reside in socially disorganized high crime areas where they have the greatest risk of coming into contact with criminal offenders, irrespective of their own behavior or lifestyle. It presupposes a correlation between staying in a crime endemic environment and becoming victim of crime. In this sense, living in a globalized world where information and communication technology hold sway has implicated most individuals as potential victims of cybercrime irrespective of their behaviours or lifestyles. The more often victims visit dangerous places, the more likely they will be exposed to crime and violence. Neighborhood crime levels, then, may be more important for determining the chances of victimization than individual characteristics. Deviant places, in this sense, include the Internet, websites, social media, email, densely populated, highly transient neighborhoods in which commercial and residential property exist side by side (Wright & Rossi, 1983; Kleck & Gertz, 1998).

Research Methodology

A cross-sectional variant of survey design was adopted- using a questionnaire as the primary data collection instrument, and supplemented it with an in-depth interview. The study area was Umuahia North Local Government Area of Abia State. It is located within the coordinates of 5°32′N 7°29′E/5.533°N 7.483°E (Umuahia, 2017). The scope of the study covered the factors of information security vulnerability as measured by the lived experiences of the Internet users in Umuahia North LGA, Abia State of South-eastern Nigeria, using data from the potential Internet users residing in Umuahia Urban part of the Umuahia North LGA, Abia State, Nigeria. Umuahia North was selected as the study area as it is a state capital, and it hosts public facilities and financial institutions that attract both cyber-criminals and cybercrime victims alike.

Internet users aged 20 to 70 years in Umuahia North Local Government Area of Abia State were the target population for this study, comprising a total of 223,134; of which 112,595 were males (50.5%) and 110,539 were females (49.5%) (National Population Census, 2006).

The sample size of 1,111 was initially selected based on published sample tables (see appendix); however, the sample size of 1,104 was selected based on the sampling procedure (see the section on sampling procedure below). According to the published tables, under the error margin or desired level of precision of ±3, any population size above 100,000 amounts to the sample size of 1,111; recall that the population size of the

study area was put at 223,134 (National Population Census, 2006). To supplement the quantitative data, 12 participants - 2 persons per ward - were selected for an in-depth interview.

The probability sampling technique was adopted to obtain the study sample. Multistage cluster and random sampling techniques were adopted (Babbie, 2008, p. 228, & 233-234). At the first stage, the primary sampling unit, Umuahia Urban was clustered into six wards of: Ibeku East I, Ibeku East II, Ndume, Umuahia Urban I, Umuahia Urban II, and Umuahia Urban III. At the second stage, polling units containing 148 housing units each in the six wards were listed. A systematic sampling technique with a random start was utilized to select four polling units each- totaling 24 polling units. At the third stage, since there was no comprehensive list or sampling frame of both housing units and households, unlike in the preceding stages, a random sampling technique was utilized in selecting 46 housing units from each of the 24 selected polling units- totaling 1,104 housing units. At the final stage, the random sampling technique was equally utilized to select a respondent from each housing unit until the 1104 sample size was completed. Only housing units containing two or more respondents were qualified to be sampled. Data in this study were collected through questionnaires and in-depth interviews (see the appendices). The primary data were analyzed using relevant descriptive and inferential statistics from the SPSS software version 23.

Socio-Demographic Characteristics of Respondents

From the socio-demographic data, the result shows that more females (50.8) than males (49.2%); more single (62.8%) than married (37.2%) participated in the survey. Again, a little above half (54.9%) of the participants were young; two-thirds (33.6%) were middle-aged, while very few (5.4%) of the old segment of the population participated. Almost all the participants were Christians (98.5%), while other religious adherents like Islam, African Religion, and Atheists rarely participated as they constituted less than 2%. About 3 in every 5 participants (58.9%) were highly educated: constituting the modal education category. 2 in 5 (40.5%) were middle educated participants, while very few of the less-educated (0.6%). Again, almost half of the participants (48.2%) were in the working-class group; followed by almost two-fifth (38.0%) who were students; with unemployed and self-employed being poorly represented as they were less than 10%.

Internet penetration was measured based on the frequency and purpose of internet usage, device used, name of service provider, types of online account operated, and the one mostly visited. The respondents were asked the following: “Could you please say how often you use the Internet facilities? a. Severally times in a day, b. Few times in a day, c. About once

in a day, d. About once in every two days, e. About once in every three or more days, f. About twice in a week, g. About three times or more in a week, h.Others, please say…". "What do you usually use the Internet for? a. For social media related activities, b. Checking and sending email, c. Google search/browsing, d. Watching film/sports, e. Others (Please say)…"What are the internet/ICT enabled devices you own/operate (circle all that applies)? a.Phone, b. Computer/Laptop, c. iPod, d. Others, please say…". "What are the online accounts do you operate (circle all that apply)? a. Facebook, b. WhatsApp, c. Twitter, d. Linkedi, e. Internet banking, f. Email, h. Instagram, g. Others, please say…". "Which of the accounts above do you visit mostly…?".

In measuring victimization, respondents were asked: "which of the following experience(s) have you had in the last 3 years? (please, circle all that apply)". "My online account(s) (Eg.email, facebook, twitter, instagram, or bank mobile App) has been hacked".; "I have complied with strange email or call asking me to disclose my personal information, like password, or BVN"; "I have lost money to stranger I met online, or through phone/email"; "I have opened/replied spam mail(s)"; "I have received email/text/call that threatened/insulted me"; "I have visited a stranger I met online and had an ugly experience"; "My computer/phone has been attacked by malware/ virus"; "I have been contacted by criminal gangs to join them"; "My computer/phone/ICT gadget(s) has been stolen/damaged"; and "I have been contacted for sexual related activities".

Respondents were regarded to have been victimized of cybercrime if they marked or describe any of the cybercrime victimization indexes in item above (all the indexes are equally weighted; and attract 1 score each), and this was coded as '1' under the 'value column' in the row of 'cybercrime victimization status' in the variable view of SPSS software (this is for categorical data).

On the other hand, respondents were regarded as not victimized if they could not describe any of the indexes above, and this was coded as '0' under the 'value column' in the row of 'victimization status' in the variable view of SPSS software (for categorical data); and this was also scored as '0' for a given participant (for the scale data).

Pattern of Internet Penetration and ICT Gadget Ownership in Abia State, Nigeria

Table 1 below shows that smart phone (61%) and computer (33%) were the most significant ICT gadgets owned by participants. Meanwhile, there were very few (<10%) that owned IPods and Tablets.

The Pattern of Internet penetration/ICT Gadget Ownership

Table 1

ICT Gadgets Owned by Participants

ICT gadgets owned by participants	N	%
Smart phone	897	61
Computer	482	33
Ipods	70	5
Tablets	12	1
Total	1,461	100

Furthermore, ownership of ICT gadgets was broadly categorized into: ownership of only smart phone and ownership of smart phone and others as shown in figure 1 below:

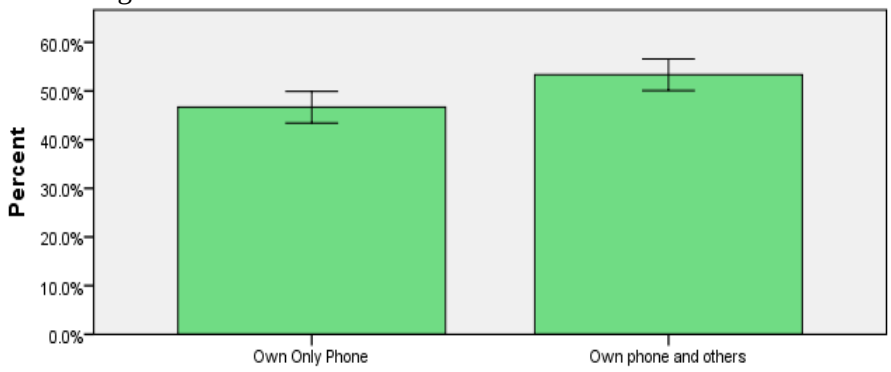

Figure 1. Bar chart describing the pattern of ICT gadget ownership**.**

As garnered from Figure 1 above, more than half (53.3%) of the respondents owned smart phone and other gadgets; while less than half (46.7%) owned only smart phones.

We summarize as follow:

1) That smart phone (61%) and computer (33%) were the most significant ICT gadgets owned by participants. Meanwhile, there were very few (<10%) that owned IPods and Tablets.
2) That more than half (53.3%) of the respondents owned smart phone and other gadgets; while less than half (46.7%) owned only smart phones.
3) That on average, participants who own smart phone and other gadgets tend to experience more cyberattacks (M = 2.53, $S.D$ = 1.63) than those who own only smart phones (M = 2.17, $S.D$ = 1.41), $t(923) = 3.453$, $p < .05$, $r = .11$. This was also confirmed by the qualitative data: all the research subjects interviewed, except one, owned smart phone and other

ICT gadgets like IPods, laptops, and others; and almost all experienced cybercrime victimization as well.

4) That Facebook (24%) and Whatssap (23%) were the most significant operated online accounts; followed by email (19%), Instagram (11%), and Internet banking (10.8%). However, Twitter, Linkedi, SnapChatt were the least operated online accounts as their proportion hovered between 7.7% and 0.6%.
5) That about 4 in every 5 of the participants operated more than one online accounts; while less than one-fifth either operated no account or owned only one account. This shows that most participants operated more than one accounts. This was also in synch with the results from the IDI section: all the subjects interviewed had multiple online accounts.

Online Account Ownership and Cybercrime Victimization in Abia State, Nigeria

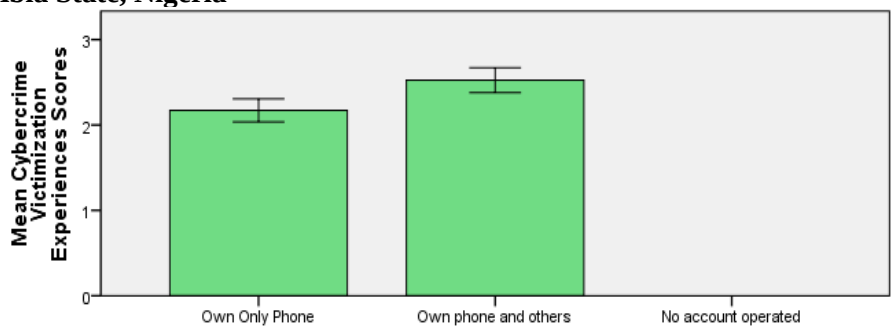

Figure 2. Bar chart describing gadget ownership and cybercrime victimization**.**

Figure 2 shows that on average, participants who own smart phone and other gadgets tend to experience more cyberattacks (M = 2.53, $S.D$ = 1.63) than those who own only smart phones (M = 2.17, $S.D$ = 1.41), $t(923) = 3.453$, $p < .05$, r = .11. This was also confirmed by the qualitative data: all the research subjects interviewed, except one, owned smart phone and other ICT gadgets like IPods, laptops, and others; and almost all experienced cybercrime victimization as well.

Table 2
Distribution of online account ownership

Online accounts participants owned	N	%
Facebook	778	24
Whatsaap	750	23
Twitter	252	7.7
Internet banking	356	10.8
Linkedi	126	3.8
Email	636	19
Instagram	372	11
SnapChatt	20	0.6
Total	3,290	100

Table 2 shows that Facebook (24%) and Whatssap (23%) were the most significant operated online accounts; followed by email (19%), Instagram (11%), and Internet banking (10.8%). However, Twitter, Linkedi, SnapChatt were the least operated online accounts as their proportion hovered between 7.7% and 0.6%.

What is more, online account ownership was broadly categorized into: ownership of only one account, ownership of multiple accounts, and ownership of no account; as figure 3 below reveals.

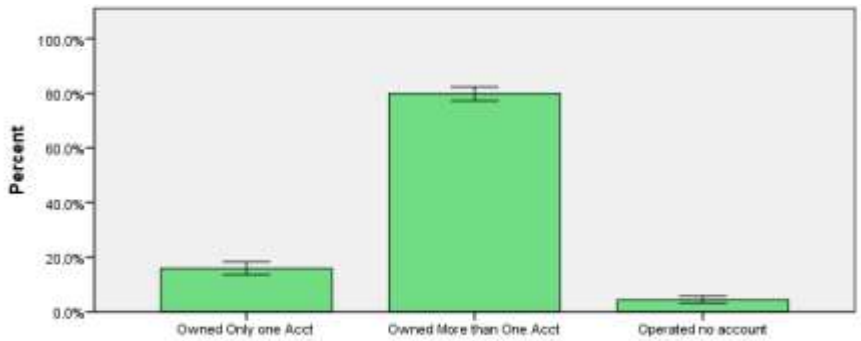

Figure 3. Bar chart showing the pattern of online account operated**.**

Figure 3 shows that about 4 in every 5 of the participants operated more than one online accounts; while less than one-fifth either operated no account or owned only one account. This shows that most participants operated more than one accounts. This was also in synch with the results from the IDI section: all the subjects interviewed had multiple online accounts.

Cybercrime Victimization by Internet Penetration/Online Account Ownership

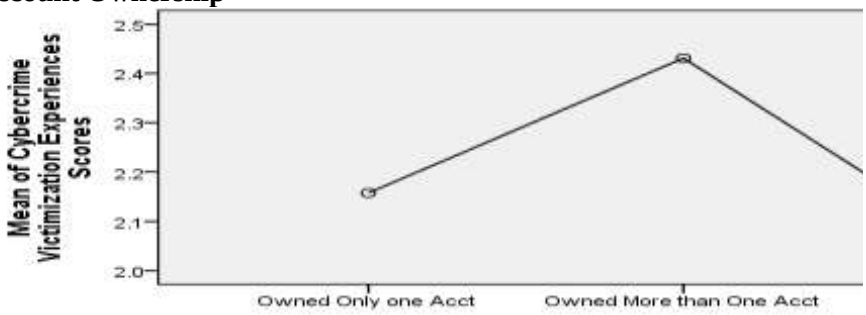

Figure 4. Mean curve description of online account ownership and cybercrime victimization experiences.

From figure 4, on average, participants who operated/owned more than one accounts are more vulnerable to cyber security incidents (M = 2.43) than those operated only one account (M = 2.16) and those operated no account at all (M = 2. 03), $f(923) = 2.889$, $p = .05$, $r = .10$. This result was also validated by the qualitative data in the sense that the subject interviewed owned multiple online accounts, and all were equally victimized. For instance, one of the participants said "I have several online accounts like Google scholar, Research gate, Facebook, Whatsaap, Linkedi, Twitter, Instagram, emails, even online banking accounts".

1) On average, participants who operated/owned more than one accounts are more vulnerable to cyber security incidents (M = 2.43) than those operated only one account (M = 2.16) and those operated no account at all (M = 2. 03), $f(923) = 2.889$, $p = .05$, $r = .10$. This result was also validated by the qualitative data in the sense that the subject interviewed owned multiple online accounts, and all were equally victimized.

Our finding majorly revealed that the Internet penetration in Abia State is really high in the sense that more people owned smart phone and other gadgets as well as operated more than one online account like Facebook and WhatsApp; and such high level of Internet penetration appear to have appear to have influenced their cybercrime attacks. We therefore conclude that the level of Internet penetration in Abia State, South-Eastern Nigeria is high; and there is likelihood that such correlates with their increased cybercrime attack. The findings have therefore cleared the suspicion whether increase in Internet penetration has a correlation with the increase in incidence of cybercrime attacks. The findings are in line with the postulations of authors like Gercke (2012), Malby et al (2013), and Nzeakor (2016) who opined that the rapid expansion of computer connectivity, and the astronomical growth of the number of Internet users have influence on the prevalence of cybercrime victimization and attacks. This result is in congruence with Okpa, Adebayo, and Emmanuel (2020) who submitted that corporate organizations in Cross River, South-Southern Nigeria, with many cyber-platforms are more likely to suffer declined productivity as a result of fishing than organizations with fewer cyber-platforms. However, it must be brought to the fore that penetration is quite different from appropriate usage. By this, we mean that the issue of cybercrime attack and vulnerability does not necessarily depend on the Internet penetration, but more on awareness and exposure to risk factors. In this sense, one can still acquire and use all the available gadgets without being attacked, if adequate awareness and digital hygiene are in place. This may partially underscore the positions being canvassed by Wall (2010) and Yar (2005).

Conclusion and Recommendations

Deriving from the study findings, the study concludes that the Internet penetration in Abia State is really high in the sense that more people owned smart phone and other gadgets as well as operated more than one online account like Facebook and WhatsApp; and such high level of Internet penetration appear to have influenced their cybercrime victimization attacks. Consequently, it is recommended that relevant government organs should carry out improved and effective cybercrime awareness campaign- targeting high Internet penetrators. Improvement in individuals' digital hygiene

through awareness and other measures that make for positive behavioural changes is also recommended.

This study contributes to the better understanding of the relationship between Internet penetration and cybercrime attacks in Abia State, Nigeria. By discovering that- the Internet penetration in Abia State is really high in the sense that more people owned smart phone and other gadgets as well as operated more than one online account like Facebook and WhatsApp; and that such high level of Internet penetration appear to have influenced their cybercrime attacks- interventions could be implemented towards increasing cybercrime awareness campaign, especially among the high Internet penetrators. Interventions could also be targeted at improving people's digital hygiene through awareness and other measures that make for positive digital behavioural change. Results of the study agree with the deviant place theory (Wright & Rossi, 1983; Kleck & Gertz, 1998) which holds that as people get exposed to dangerous places, the more likely people would become victims of crime and violence. In accordance with the ideals of the theory, cybercrime victims do not encourage cybercrime but are victim-prone because they reside in society with high Internet penetration where they have the greatest risk of coming into contact with cyber-criminal offenders. In this sense, irrespective of their own behavior or lifestyle, victims may still become cybercrime victims. This is exactly the case with Internet users in Abia State who experience cybercrime attacks

References

Akuta, E. A. M., Ong'oa, I. M., & Jones, C. R. (2011). Combating cybercrime in Sub-Sahara Africa: A discourse on law, policy and practice. *Journal of Research in Peace, Gender and Development,1(4), 129-137.*

Babbie, E. (2008). *The basics of social research* (4thed.). Belmont, USA: Thomson Wadsworth.

Boateng, R., Olumide, L., Isabalija, R. S., &Budu, J. (2011). Sakawa – Cyber crime and criminality in Ghana. *Journal of Information Technology Impact, 11(2),* 85-100.

Counterpoint. (2023). Global Smartphone Shipments 2011 – 2022. Retrievedfrom https://www.counterpointresearch.com/devices/smartphones/

Gercke, M. (2012). *Understanding cybercrime: Phenomenon, challenge and legal response*. Geneva: International Telecommunication Union (ITU).

Hansen, J. R. (2007). Cybercrime prevention. In K. O'Shea, J. Steete, J. R. Hansen, C. B. R.

Jean, & T. Ralgh (Eds). *Cybercrime investigations: Bridging the gaps between security professionals, law enforcements and prosecutors* (pp. 261-283). New York: SynGress Publishing.

Haralambos, M., and Holborn, M. (2008). *Sociology: Themes and perspectives* (7thEd.). London: HarperCollings Publishers.

Internet. (2012). World Internetstats. Retrieved from http://www.internetworldstats.com/stats.htm.

Internet crime complaint center (2016) Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Internet crime complaint center (2021) Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Jaishankar, K. (2010). Editorial – The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology*, 4 (1&2), 26 -31.

Kleck, G., & Gertz, M. (1998). Carry guns for protection: Results from the national self-defense survey. *Journal of Research in Crime and Delinquency* 35: 193–224.

Lee, G., & Sanchez, M. (2018). Cyber bullying behaviours, anonymity, and general strain theory: A study of undergraduate students at South Eastern University in the United States. *International Journal of cyber Criminology, Vol.12 (1*).

Leukfeldt, R., Veenstra, S., &Stol, W (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, *7*(1), 1–17.

Liebel, D. (2013). The watch dog: Do you know the superagency that can best protect you from cyber crimes? Retrieved from http://www.dallasnews.com.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., &Ignatuschtschenko, E. (2013). *Comprehensive study on cybercrime*. Vienna: United Nations Office on Drugs and Crime.

Mali, P. (2008). Cyber law consulting: Text book of cybercrime and penalties. Retrieved fromwww.cyberlawconsulting.com.

Moulton, M. (2010). *The future of cybercrime*. In T. Finnie, T. Petee, & J. Jarvis (Eds), Future challenges of cybercrime (74-76). Virginia: Futures Working Group.

National Population Commission. (2006). State population: Abia final. Retrieved from www.population.gov.ng.

Nwoke, C. N., Nzeakor, O. F., Nwoha, N. G., Ugwu, O., Uba-Uzoagwa, O. P. & Ikenegbu, T. (2021). Determinants of Cybercrime Awareness among Internet users in Nigeria". *International Journal of Humanities and Social Science, Vol. 8 (5),* September 2021: 14-22.

Nzeakor O. F. Nwoha, N. G. & Nwoke, C. N. (2022). Cybercrime awareness and cybercrime
victimization in Imo state, Nigeria**".** *FUWukari Vol. 1, Issue 1,* pp 147 – 162.

Nzeakor, O. F., Nwokeoma, B. N., Hassan I., Ajah B. O., & Okpa, J. T. (2022). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity, Intelligence & Cybercrime. Vol. 5, Issue 3*, pp 41-67. https://vc.bridgew.edu/ijcic.

Nzeakor, O. F. (2021). Cyber-criminality and experiences of Internet users in Abia State of South-Eastern Nigeria. A Ph.D dissertation presented to the department of Sociology and Anthropology, University of Nigeria, Nsukka.

Nzeakor, O. F. (2016). Awareness of cyber policing among tertiary institutions in Imo State. An M.Sc thesis presented to the department of Sociology and Anthropology, University of Nigeria, Nsukka.

Nzeakor, O. F, Nwokeoma, B. N., & Ezeh, P-J. (2020). Ezeh "Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. *International Journal for Cyber criminology*, *Volume 14, Issue 1*, January – June. Retrieved from http://www.cybercrimejournal.com.

Olusola, M., Ogunlere, S., & Semiu, A. (2013). Impact of cybercrimes on Nigerian economy.

Babcock University. Retrieved from https://www.vanguardngr.com /2017/05/450m-lost-cyber-crime-nigeria-senate/

Okpa, J. T., Adebayo, I. A., & Emmanuel, E. (2020). Cybercrime and socioeconomic development of corporate organizations in Cross River State, Nigeria. *Asian Journal of Scientific Reseach, 13*: 205-213. DOI: 10.3923/ajsr.2020.205.213.

Okpa, J. T, Ajah, B. O., Nzeakor, O. F., Eshiotse, E, & Abang T. A. (2022). Business E-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*. https://doi.org/10.1057/s41284-022- 00354-1

Siegel, L. J. (2010). *Criminology: Theories, patterns, and typologies.* (10th ed.). Belmont, USA: Wadsworth Cengage Learning.

Statista. (2023). Number of internet users worldwide from 2005 to 2022. Retrieved from https://www.statista.com.

The current state of cybercrime. (2013). An inside look at the changing threat landscape. Retrieved from http:// www.rsa.com.

Ugwuoke, C. U. (2010). *Criminology: Explaining crime in the Nigerian context*. Nsukka: Great AP Express Publishers.

Umuahia (2017). Retrieved from https://en.m.wikipedia.org/wiki/Umuahia

Wada, F., & Odualaja, G. O. (2012). Assessing cybercrime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT, 5(1), 69-82*.

Wall, D. S. (2010). Foreword. In K. Jaishankar (Ed.). *Cyber criminology: Exploring Internet crimes and criminal behavior*. London: CRC Press.

Warren, P., & Streeter, M. (2005). *Cyber alert: How the world is under attack from a new form of crime*. London: Vision Paperbacks.

Webroot Threat Report (2020). 2020 Webroot Threat Report: Phishing Attempts Grew by 640% Last Yearhttps. Retrieved from https://s23.q4cdn.com/197378439/ files/doc_news/archive/6f77d7f0-f129-4da6-bafe-0515e728aedd.pd.

Wright, J., & Rossi, P. (1983). *Armed and considered dangerous: A Survey of felons and their firearms.* Hawthorne, NY: Aldine De Gruyter.

Yar, M. (2005). The novelty of cybercrime: An assessment in Light of routine activity theory. *European Journal of Criminology*. *2*(4), 407-427. doi: 10.1177/147737080556056.