International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 3 Article 4

11-1-2022

Emerging Trends in Cybercrime Awareness in Nigeria

Information Security, Awareness, Cybercrime, Victimization, Awareness Categories, Property and Violent Cybercrime

Nzeakor et al. (2022). *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(3), 41-67.

Emerging trends in cybercrime awareness in Nigeria

Ogochukwu Favour Nzeakor*, Ph.D., Michael Okpara University of Agriculture, Nigeria
Bonaventure N. Nwokeoma, Ph.D., University of Nsukka, Nigeria
Ibrahim Muhammad Hassan, M.Sc., Niger State College of Education, Nigeria
Benjamin Okorie Ajah, Ph.D., University of Nsukka, Nigeria
John Thomson Okpa, Ph.D., University of Calabar, Nigeria

Keywords: Information Security, Awareness, Cybercrime, Victimization, Awareness Categories, Property and Violent Cybercrime

Abstract:
The study examined the current trend in cybercrime awareness and the relationship such trend has with cybercrime vulnerability or victimization. Selecting a sample of 1104 Internet users from Umuahia, Abia State, Nigeria, We found that: 1) awareness of information security was high in that about 2 in every 3 (68%) participants demonstrated a favorable awareness of information security and cybercrime. It was, however, revealed that such a high level of awareness could be partial and weak. 2) most Internet users demonstrated the awareness of fraud-related cybercrime categories (39%), e-theft (15%), hacking (12%), and ATM theft (10%). However, they were rarely aware of sexually related offenses, cyber-terrorism, malware attacks, spam emails, and identity theft as their proportion hovered around 8% and below. 3) Internet users significantly demonstrated more awareness of computer-assisted (M = 2.5; SD = 1.7) than that of computer-focused cybercrime categories (M = 2.2, SD = 1.3), t(1103) = 2.9, p=.000, r =.2. 4) Internet users significantly demonstrated more awareness of property cybercrime (M = 2.54; SD = 1.6) than that of violent cybercrime categories (M = 1.82, SD = 1.2), t(1103) = 5.94, p=.000, r =.3. 5) cybercrime awareness is positively correlated to cybercrime victimization experiences in that participants who demonstrated more awareness of cybercrime experienced significantly more cybercrime victimization (M = 1.66; SD = 1.7) than those who did not demonstrate awareness of cybercrime (M = .73, SD = 1.4), t(1103) = 7.55, p=.000, r =.52.

Introduction

The globalized world now exposes individuals to all manner of vulnerability that is not constrained by the usual barriers of physical distance. Indeed, even if one does not use the Internet, much of his/her personal information is possibly stored somewhere on a networked computer (Yar, 2005). So, by all means, every individual is a potential victim of cybercrime (Nzeakor et al., 2020). The above implication is that cybercrime victimization is now a global social problem: defying several mitigating measures. Internet-enabled crimes and scams have shown no sign of letting up, as the 2019 report of the Internet Crime Complaint Center indicates (Wall, 2010; Ndubueze, 2017; Rich, 2010; Internet Crime Complaint Center, 2019).

Cybercrime is conceptualized as illegal activities committed using a 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-pedophiles, and e-sexual grooming. On the other hand, cybercrime awareness is conceptualized, in this study, as having appreciable knowledge of diverse criminal activities or computer security incidents on the Internet.

Studies have attributed the increasing spate of cybercrime and vulnerability of Internet users to several factors. One of Such factors is the fact that such Internet users in many cases are not even aware of the

*Corresponding author
Ogochukwu Favour Nzeakor*, Ph.D., Peace & Conflict Unit, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria
Email: nzeakor.ogochukwu@mouau.edu.ng

risks of using the Internet and often venture into cyberspace vulnerably (Kritzinger & von Solms, 2010; Zhang et al., 2009; Liebel, 2013; Malby et al., 2013; Nzeakor, 2016; Nzeakor et al., 2020).

Furthermore, many studies have advanced that cybercrime or information security awareness is one of the defenses against the continuously evolving threat landscape and a way to mitigate security attacks (Siponen & Oinas-Kukkonen, 2007; Tsohou et al., 2008; Aloul, 2012). It has equally been argued that despite the undertaken approaches and the use of security tools, humans remain the weakest link in information system security regarding the incidents they result in and the costs incurred (Aurigemma et at., 2012). In the same way, Joinson and colleagues found that despite the increasing level of penetration of technology in everyday life, individuals' behaviors concerning protecting their privacy have not progressed at the same pace (2010). In this sense, cybercrime information security awareness enables users to understand their role in the security process and encourages them to take necessary measures for their peer's information security (Amankwa et al., 2014).

Meanwhile, several studies have identified the factors and challenges of increasing cyber-security awareness. One of such factors identified by researchers is the factor or issue of low prevalence or volume of cybercrime awareness (Hansen, 2007; Malby et al., 2013; Sasse et al., 2001; Leukfeldt et al., 2013; Mylonas et al., 2013). For instance, Mylonas and colleagues found that users of smartphones, one of the most commonly used information and communication technology (ICT) devices, lack security awareness and are not adequately prepared to make appropriate security decisions (2013). Leukfeldt and colleagues concluded that the first problem in detecting and investigating cybercrime in Singapore is that victims of cybercrime do not always notice that they are being victimized (2013).

However, other researchers argued that the problem was more of quality or content and less of the volume of awareness (Utcu & Testik, 2015; Nzeakor et al., 2020). For instance, Nzeakor and colleagues found that although the awareness level was relatively high in Nigeria, it was superficial because the Internet users were more aware of computer-assisted than computer-focused cybercrime categories (2020). In the same token, Utcu and Testik argued that increasing awareness level has not corresponded with increasing relevant defensive behavior (2015).

Apart from the wide gap between knowledge and good practices, other studies have identified psychological, technical, and economic factors to cyber-security or cybercrime awareness. Malby and colleagues discovered that despite a growing number of cybercrime awareness campaigns, some countries reported it would take a while for the public awareness campaigns to build public trust (2013). Receiving information about cybercrime did not necessarily translate into 'feeling informed' about cybercrime or cyber-security. The study also highlighted other challenges in developing appropriate and cost-effective campaigns, providing information to users without additional training and skills acquisition activities. The study equally concluded that simple campaigns focused on a specific target group seemed to be most cost-effective. There are also limits to how far users can be expected to learn complex security mechanisms, remember long and varied passwords for every online service they sign up to, and take other precautions that often directly interfere with the task at hand (Sasse et al., 2001).

Therefore, it can be deduced from the above that the current trend in information or cyber-security awareness appears very vague in the literature. Again, very few studies are dedicated to Nigeria's information security or cybercrime awareness. In this regard, the knowledge of the pattern of information security awareness,

or even the categories of cybercrime Internet users in Nigeria, is still nascent and under-researched. This, therefore, raises some salient questions as to the individual awareness of the categories of cybercrime. Does the pattern of awareness have any relationship with the individuals' cybercrime vulnerability or victimization? We believe that answering these questions would contribute immensely to the policies and interventions to improve the quality of cybercrime awareness campaigns and reduce the spate of cybercrime vulnerability both in Nigeria and globally.

Study Objectives

The central aim of the study is to examine the current trend in cybercrime or information security awareness and the relationship such trend has with cybercrime vulnerability or victimization. The specific objectives are the following: (1) To ascertain the level of cybercrime awareness; (2) To examine categories of cybercrime awareness; and (3) To investigate the relationship between cybercrime awareness patterns and cybercrime victimization experiences.

Research Hypotheses

H1: Internet users who demonstrated more awareness of computer-assisted cybercrime tend to experience more cybercrime victimization than those who demonstrated more awareness of computer-focused cybercrime categories.
H2: Internet users who demonstrated more awareness of property cybercrime categories tend to experience more cybercrime victimization than those who demonstrated more awareness of violent cybercrime categories, trolling, airing dirty laundry, public shaming).

Literature Review

The Trend in Information/Cybercrime Awareness

As observed by Zhang and colleagues, past research on information systems (IS) or cyber-security tends to emphasize the role of information security awareness in information system security or the control of cyber security incidents (2009). The emphasis is on end-user security, organizational factors, and security behaviors with user actions that influence information systems' confidentiality, integrity, and availability (Stanton et al., 2005). Incorporating perceived technical security protection into the theory of planned behavior and examining factors affecting end-user security behaviors (Zhang et al., 2009).

Other studies on information security or cybercrime awareness have emphasized psychological, technical and economic factors (see Malby et al., 2013; Sasse et al., 2001; Rich, 2010; Hadlington et al., 2020). Hadlington and colleagues, for instance, examined the factor of the "fear of missing out" (2020). Malby et al. (2013) worked on the means and modes of carrying out effective anti-cybercrime awareness campaigns Sasse, Brostoff and Weirich (2001), Rich (2010), and AlMindeel and Martins (2020) concerned themselves with the inherent weaknesses with information security awareness dissemination, Gercke (2012), and Nzeakor et al. (2020) examined the pattern and prevalence of cybercrime awareness.

A closer examination of the above narrative reveals that the trend in cybercrime awareness from African or Nigerian backgrounds is arguably under-researched. For instance, although researchers have examined

the inherent weaknesses with information security awareness dissemination using data from outside Nigeria, literature is still in the dark regarding trends from Nigerian backgrounds (Sasse et al., 2011; Rich, 2010). In this vein, Malby and colleagues relied on data from outside Nigeria to describe the features of effective cybercrime awareness campaigns at the global level (Malby et al., 2013). Hadlington and colleagues linked a low volume of information security or cybercrime awareness with the increasing prevalence of "fear of missing out" among some selected Saudi Arabian employees (2020). Hadlington et al. (2020)'s findings revealed nothing regarding the situation in Africa. Ogutcu and others (2015) analyzed the personal information security behavior and awareness of 881 information users and found that: the more the respondents perceive threats, their behavior becomes more protective; students, compared to other groups, are more vulnerable against risks, and the education level and information security awareness are positively correlated (Ogutcu, et al., 2015).

Given that social phenomena are contextual and dissimilar, it would make policy and empirical sense to examine the current trend in cybercrime awareness from a Nigerian background.

Categories of Cybercrime Awareness

In light of the challenges associated with the definition of cybercrime, its awareness, or victimization, most scholars prefer categorizing rather than defining it (Nzeakor et al., 2020). For instance, the 2005 Council of Europe Convention on Cybercrime categorized cybercrime or its awareness into four offenses: offenses against confidentiality, integrity, and availability of computer data and systems; content-related offenses; copyright-related offenses; and computer-related offenses. Researchers prefer broad and binary categorization of cybercrime awareness for computer-assisted and computer-focused cybercrimes and cybercrime awareness (Ashaolu, 2011; Gordon & Ford, 2006; Yar, 2005).

Computer-assisted cybercrime awareness. These refer to the demonstration of sufficient knowledge or awareness of such categories of cybercrime that pre-date the Internet but take on a new life in cyberspace. They include cyber terrorism; e-forgery; e-fraud; identity theft; erotic and pornographic material, e-pedophile; racism, hate speech, glorification of violence; religious offenses; illegal gambling and online games; libel and false information; cyberbullying; cyber stalking; copyright-related offences; trademark-related offenses; and e-drug trafficking (Ashaolu, 2011; Gordon & Ford, 2006; Yar, 2005; Mbachu & Nazeef, 2017).

Computer-focused cybercrime awareness. These refer to the demonstration of sufficient knowledge or awareness of such categories of cybercrime that have emerged in tandem with the establishment of the Internet and could not exist apart from it. They include ransom-worms; email bombing; denial-of-service attack; trojan; key-loggers; remote administration tools; spam; ransomware; logic bombs; botnets; exploit kits; hacking; data espionage; illegal interception; data/system interference; viral attacks; phishing; email/web spoofing; and web jacking (Ashaolu, 2011; Gordon & Ford, 2006; Yar, 2005; Mbachu & Nazeef, 2017).

Information Security/Cybercrime Awareness and Cybercrime Victimization

Although a good number of scholars are of the consensus that increasing the awareness of the cybercrime scourge holds better promise in cyber-policing (Boateng et al., 2011; Liebel, 2013; Leukfeldt et al., 2013; Hansen, 2007), there is still some twist with the awareness as a strategy. For instance, Nzeakor and

colleagues observed that although some studies have advanced possible relationships between cybercrime awareness and cybercrime prevention and control, there seems to be no consensus among these authors regarding the direction and strength of the relationship (2020; Gercke, 2012); Malby et al., 2013; Boateng et al., 2011; Leukfeldt et al., 2013; Lee, 2018). While some people opined that there is no relationship; some advanced a negative and strong correlation between cybercrime awareness and cybercrime victimization. People aware of the cybercrime scourge are less likely to experience cybercrime victimization. For instance, Hansen concluded that "with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, we (sic) are still vulnerable to the frailties of human behavior (2007, p.63)." Nzeakor and colleagues had conflicting results from quantitative and qualitative data on the relationship between cybercrime awareness and cybercrime victimization (2020). On the quantitative data, Nzeakor and colleagues concluded a significant positive relationship between cybercrime awareness and cybercrime victimization, while the qualitative data (from the In-depth Interview (IDI) section) found otherwise (2020). Liebel supporting a negative correlation between cybercrime awareness and cybercrime victimization opined that if someone knows that there are chances of losing their money by clicking open an email from an overseas criminal hacker and paying for an offer, they would not have done that (2013).

Theoretical framework: Routine Activities Theory and Victim Precipitation Theory

Routine Activities Theory (RAT) from Cohen and Felson (1979) and Victim Precipitation Theory from Wolfgang (1958) provided an analytical framework for the study.

Victim Precipitation Theory (VPT) was adopted to guide the study in understanding the possible contributions of the victims towards their victimization. The major postulate of the theory is that victims trigger cyber-criminality by their provocative behavior such as exposure to cybercrime risk behavior; as well other careless digital interaction as a result of ignorance; and others.

On the other hand, the Routine Activities Theory (RAT) helps explain the possible link between lack or inadequate guardianship (lack of adequate awareness) and cybercrime victimization. The central premise of the Routine Activities Theory (RAT) holds that the volume and distribution of predatory crime are closely related to the interaction of three variables that reflect the routine activities of the typical American lifestyle. However, the current information society that has made the world a global village has changed the trajectory- so it is no longer about the American lifestyle but the global lifestyle. In this sense, the theory can be adapted to explain the nature of cybercrime victimization. The volume and distribution of cybercrime information in society and the economy are closely related to the fact that data is now the mainstay of the economy and the interaction of three variables that reflect the routine activities of the typical lifestyle in the information society. Such three variables include the availability of suitable targets, the absence of capable guardians, and the presence of motivated offenders. The theory examines how cybercrime victimization and vulnerability would become inevitable whenever or wherever there is insufficient security or lack of capable guardianship (say, lack of awareness on both the side of Internet users and security personnel).

Research Methodology

Study Design

The study adopted a cross-sectional variant of survey design- using a questionnaire as the primary data collection instrument, and supplemented it with an in-depth interview. The quantitative (i.e., the questionnaire) data measured and captured the trends in awareness and its relationship with Internet vulnerability, while the qualitative data exposed their dynamics.

Area and scope of the study

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 trends in awareness and its relationship with Internet vulnerability using data from the Internet users residing in Umuahia Urban part of the Umuahia North LGA, Abia State during 2020. Umuahia was selected as the study area as it is a state capital, and it hosts public facilities and financial institutions that attract both cybercriminals and cybercrime victims alike.

Study Population

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, 112,595 males (50.5%) and 110,539 females (49.5%) (National Population Census, 2006).

Sample Size

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 Israel, several approaches to determining sample size (1992). These include using a census for small populations, imitating similar studies' sample sizes, using published tables, and applying formulas to calculate the sample size. In this study, published tables were adopted (see appendix). 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.

Sampleing Procedure

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 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 1,104 sample size was completed. Only housing units containing two or more respondents were qualified to be sampled.

Participants for the in-depth interview were selected based on the information from the retrieved questionnaire items. At the end of the questionnaire, an appeal read, "kindly drop your contact if you would not mind a further discussion of your experience(s) with the researcher". Participants who complied were further "sifted" how many times they were victimized and their ward location- by so doing, 12 participants from the six wards were selected.

Data collection

We adopted a questionnaire as the primary instrument and in-depth interview guides as an auxiliary instrument (see the appendices).

Data processing and analysis

The field data were analyzed using relevant descriptive and inferential statistics from the SPSS software version 23.

Participants

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%.

Variable and concept definition

Awareness of cybercrime/information security. This study is operationalized as having appreciable knowledge of diverse criminal activities or computer security incidents on the Internet. Participants' cybercrime and information security awareness status were measured by asking the following questions in the questionnaire items: 'Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM?'; 'If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years. Participants were regarded as aware of cybercrime if they could mention or describe at least one category of cybercrime e-fraud.

Awareness of computer-assisted cybercrime categories. This was described as the demonstration of awareness of those cybercrime categories that pre-date the Internet but take on a new life in cyberspace. Such categories include cyber terrorism; e-forgery; e-fraud; identity theft; and erotic and pornographic material (Ashaolu, 2011; Gordon & Ford, 2006; Yar, 2005; Mbachu & Nazeef, 2017).

Awareness of computer-focused cybercrime awareness categories. This could be described as the demonstration of awareness of those cybercrime categories that have emerged in tandem with the establishment of the Internet and could not exist apart from it. Such categories include ransom-worms, email bombing, denial-of-service attack, trojan, key-loggers, remote administration tools, and others (Ashaolu, 2011; Gordon & Ford, 2006; Yar, 2005; Mbachu & Nazeef, 2017).

Awareness of property cybercrime categories. This refers to demonstrating awareness of those cybercrimes where an offender attempts to steal or damage an object directly. They include e-fraud, e-theft, hacking, data espionage, illegal interception, data and system interference, viral attacks, and phishing. The target here is property- whether cash or other materials.

Awareness of violent cybercrime categories. This could be the demonstration of awareness of those online criminal acts in which death or physical injury results, for example, awareness of e-rape and other online pornographic offenses, e-stalking, and e-bullying.

Cybercrime. It is also known as "computer security incidents." It refers to illegal activities committed using a 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-pedophiles, and e-sexual grooming.

Partial. cybercrime awareness: It is operationally defined as Internet users whose awareness of cybercrime is incomplete, are only limited to their experience and are inadequate to protect them from exposure and victimization.

Results

Objective 1: To ascertain the level of cybercrime awareness

Respondents were asked: "Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM?" "If yes, please mention or describe the one(s) you know people have suffered on the Internet in the last three years." Awareness of cybercrime was therefore measured by not only circling "yes," but by mentioning or describing a given cybercrime category- say "spam mail" or "fraud." What is more, the level and prevalence of cybercrime awareness were considered very low when M < 0.5 or <30%; moderate when M ≥0.5 or 40%; high when M ≥ 1 or 60%; and considered very high when M >2 or 70%.

Table 1 shows that about 2 in every 3 (68%) participants demonstrated a favorable awareness of information security and cybercrime, as against about one in three participants (32%) that did not demonstrate a favorable awareness of cybercrime (M= 1, SD=87). It, therefore, implies that awareness of information security was favorably high (M ≥ 1 or 60%) in Abia State, Nigeria.

Table 1. Participants' Cybercrime Awareness Status/Level

Cybercrime Awareness Status	N	%
Aware	755	68
Not aware	349	32
Total	1104	100

Objective 2(a): To examine categories of cybercrime awareness

Table 2. Categories of Cybercrime Awareness

Categories of cybercrime awareness	N	%
Hacking	88	12
E-fraud	297	39
E-theft	110	15
Responding to spam emails	3	0.4
Online facilitated murder	25	3
Online facilitated kidnapping	17	2
Viral/malware attacks	3	0.4
Online sexual-related offenses/sexting	64	8
Business email compromise	14	2
Online bullying/blackmail	27	4
Identity theft	16	2
ATM-related theft	78	10
Online facilitated money ritual	10	1
Cyber-Terrorism	3	0.4
Total	755	100

From Table 2, it was revealed that while most Internet users demonstrated the awareness of fraud-related cybercrime categories (39%), e-theft (15%), hacking (12%), and ATM theft (10%); Internet users were rarely aware of sexually related offenses, cyber-terrorism, malware attacks, and spam emails, as their proportion hovered around 8% and below.

Furthermore, as revealed from the literature, some authors have attempted a binary categorization of cyber security incidents and cybercrime and its awareness into computer-focused and computer-assisted. Other categories of authors, especially from Africa, equally attempted another binary categorization based on predatory crime. In this regard, cybercrime and its awareness are divided into violent and property cybercrime categories.

Objective 2(b): To discover the mean difference in participants' awareness of computer-focused and computer-assisted cybercrime categories

Table 3 reveals that Internet users significantly demonstrated more awareness of computer-assisted ($M = 2.5$; $SD = 1.7$) than that of computer-focused cybercrime categories ($M = 2.2$, $SD = 1.3$), $t(1103) = 2.9$, $p=.000$, $r =.2$. Therefore, more participants are likely to be abreast of computer-assisted cybercrime categories

like e-fraud or e-theft than computer-focused categories like spam or virus attacks. In revealing the possibility of this, a participant from the IDI section (Participant No. 11) put it thus: "yes, I know of online duping because I recently fell victim to that."

Table 3. Differences in the Scores of Computer-Focused and Computer-Assisted Awareness Categories

Categories of Cybercrime Awareness	n	Mean	SD	t	p
Computer-Assisted	1104	2.5	1.7		
Computer-Focused	1104	2.5	1.7	2.49	**

*Notes: **p<.01. *p<.05.*

Objective 2(c): To discover the mean difference in participants' awareness of computer-focused and computer-assisted cybercrime categories

Table 4. The difference in the scores of violent and property categories of cybercrime awareness

Categories of Cybercrime Awareness	n	Mean	SD	t	p
Computer-Assisted	1104	2.54	1.6		
Computer-Focused	1104	1.82	1.2	5.94	**

*Notes: **p<.01. *p<.05.*

The results from the t-test indicate that Internet users significantly demonstrated more awareness of property cybercrime (M = 2.54; SD = 1.6) that of violent cybercrime (M = 1.82, SD = 1.2), t(1103) = 5.94, p=.000, r =.3, implying that more participants are likely to be abreast of property than violent cybercrime categories.

The qualitative data conveyed the same pattern: most of the participants in the In-Depth Interview (IDI) section demonstrated more awareness of property cybercrime categories like identity theft, hacking, and business email compromise than they demonstrated the awareness of the violent category like cyber-pornography, online bullying, blackmail, and online facilitated money ritual.

Objective 3(a): To discover the mean difference in participants' awareness of computer-focused and computer-assisted cybercrime categories

Table 5. The difference in the scores of victimization experiences of participants who demonstrated awareness of cybercrime and those who did not

Cybercrime Awareness Categories	n	Mean	SD	t	p
Aware	1104	1.66	1.7		
Not Aware	1104	.73	1.4	7.55	**

*Notes: **p<.01. *p<.05.*

Table 5 shows that on average, participants who demonstrated more cybercrime awareness experienced significantly more cybercrime victimization (M = 1.66; SD = 1.7) than those who did not demonstrate awareness of cybercrime (M = .73, SD = 1.4), t(1103) = 7.55, p=.000, r =.52.

This finding implies that individuals who have experienced specific cybercrime victimization experiences are more aware of such categories experienced than other categories yet to be experienced. It is also possible that their cybercrime victimization experiences preceded their awareness and meaning they were not aware prior to their victimization experiences. The IDI data also sustained the pattern. For instance, all the interviewed participants admitted being aware of cybercrime even though they all experienced cybercrime victimization.

Objective 3(b): To ascertain the correlation between participants' victimization experiences and their awareness pattern: computer-focused and computer-assisted cybercrime categories.

Table 6. Correlation between cybercrime victimization experiences and awareness of computer-focused and computer-assisted categories

Status of Cybercrime Victimization	Computer-focused	Computer-assisted
Not Victimized	24 (11%)	19 (4%)
Victimized	202 (89%)	510 (96%)
Total	**226**	**529**

Table 6 shows that of 755 participants who demonstrated awareness of cybercrime, as high as 7 in 10 (N=529; 70%) demonstrated awareness of computer-assisted, while as low as 3 in 10 demonstrated awareness of computer-focused (N = 226; 30%). Meanwhile, of the 226 who demonstrated the awareness of computer-focused cybercrime categories, 89% experienced victimization versus just 11% who did not experience victimization. On the other hand, of 529 who demonstrated awareness of computer-assisted cybercrime, almost all (96%) experienced cybercrime victimization. Therefore, more of those who demonstrated computer-assisted awareness appear to experience victimization than those who demonstrated awareness of computer-focused categories.

Objective 3(c): To ascertain the correlation between participants' victimization experiences and their awareness pattern: computer-focused and computer-assisted cybercrime categories.

Table 7. Correlation between cybercrime victimization experiences and awareness of the property and violent cybercrime categories

Status of Victimization	Violent Cybercrime	Property Cybercrime
Not Victimized	26 (13%)	36 (6%)
Victimized	173 (87%)	520 (94%)
Total	**199**	**556**

Table 7 shows that 755 participants who demonstrated awareness of cybercrime, as high as 8 in 10 (81%) demonstrated awareness of the categories of property cybercrime. In contrast, while as low as 3 in 10 (19%) demonstrated awareness of violent cybercrime categories. Meanwhile, of the 199 who demonstrated the awareness of violent cybercrime categories, 87% experienced victimization; as against just 13% did not experience victimization.

On the other hand, of 556 who demonstrated awareness of property cybercrime, almost all (94%) experienced cybercrime victimization. 6% did not experience victimization. Thus, more of those who demonstrated

property cybercrime awareness appear to experience victimization than those who demonstrated awareness of violent cybercrime categories.

Table 8. Relationship between victimization experiences and cybercrime awareness pattern: computer-focused and computer-assisted

	Cybercrime Awareness Pattern		
Victimization Status	**Computer-Focused**	**Computer-Assisted**	**Total**
Not Victimized	24(11%)	19(4%)	43
Victimized	202(89%)	510(96%)	712
Total	**226(100%)**	**529(100%)**	**755(100%)**

Notes: $X^2 = 14.50$, p= .000, n = 755, df = 1. Row percentages are shown below observed cell counts.

Table 9. Relationship between victimization experiences and cybercrime awareness pattern: property and violent cybercrimes

Victimization Status	**Violent Cybercrime**	**Property Cybercrime**	**Total**
Not Victimized	26(13%)	36(6%)	62
Victimized	173(87%)	520(94%)	693
Total	**199(100%)**	**529(100%)**	**755(100%)**

Notes: $X^2 = 12.00$, p= .001, n = 755, df = 1. Row percentages are shown below observed cell counts.

Discussion

The central aim of the study was to examine the current trend in cybercrime or information security awareness and the relationship such trend has with cybercrime vulnerability or victimization.

The first objective was to ascertain the level of cybercrime awareness. The result shows that about 2 in every 3 (68%) participants demonstrated an awareness of information security and cybercrime. About 1 in 3 participants (32%) did not demonstrate a favorable awareness of cybercrime. It, therefore, implies that awareness of information security was favorably high ($M \geq 1$ or 60%) in Abia State, Nigeria.

However, there is a suspicion that the result of the high level of cybercrime awareness amongst the Internet users in Abia State, Nigeria, could be spurious. Further examination of the data revealed that most Internet users became informed, especially of a particular category of cybercrime, due to their victimization experiences. Their awareness is equally limited to those categories of cybercrime experienced. In reality, partial or shallow cybercrime awareness is what should be high, and it, therefore, means that a very negligible proportion of the users are aware of the cybercrime scourge. This position was strengthened because most participants from the IDI section experienced cybercrime victimization irrespective of their claim to be aware of cybercrime. The questionnaire and IDI responses indicated that most participants mentioned the same cybercrime categories for victimization and awareness.

Moreover, evidence from secondary sources supports the position of partial awareness: For instance, a Facebook user, Mike Obi, shared on his wall how he fell victim to cybercrime even when he thought he was well informed about it. He narrated his experience thus:

> *Odogwu* became *Adanma* [literally translated to mean *pundit* has *turned out to be a novice*]. Blame me if you can. Some two weeks ago, one Anderson Sharon sent me a friendship request which I accepted. Later she demanded cam chat, which I told her that my phone don't have such facility. She promised she will send me iPhone 7.' I was so delighted. Last Sunday she told me she has sent it with the waybill I shared. Monday yesterday I got a message supposedly from Lagos informing me to come and pick the parcel from Ikeja Airport. I told the caller that I am in PH. The caller told me that Arik Flight is coming to PH that I should pay #30,500 that the parcel will be hand delivered to my office. I paid into Adodo Lucky account with Gtbank. Supposedly again at PH airport a guy called Victor called to inform me that he is the one to deliver the parcel. Victor now later called to say that the parcel also contains 900 pounds. I was now being accused of money laundering. However, they can help me to clear it on payment of #100k. I requested to have an account where I can pay the #100, but it was Adodo Lucky account that was sent to me again. This raised my suspicion. After this stage others are story. Just for your caution [Content Analysis: https://www.facebook.com/obi.michea.77.

While partially in agreement with Nzeakor and colleagues who concluded that the knowledge of cybercrime menace appeared very superficial, the finding helps sharpen or put other findings into perspective (2020; Kazeem, 2019; Boateng et al., 2011). For instance, Boateng et al. (2011) found that cybercrime awareness was on the increase in Ghana; however, in the light of the extant finding, what was actually in an increase in Ghana was partial awareness (i.e., awareness of cybercrime that is incomplete, and only limited to those categories of cybercrime victims experienced). In the same way, shallowness in the Internet users' awareness status is better hinged on the ground that Internet users are more aware of those categories of cybercrime they have experienced than those not experienced. This finding contradicts Nzeakor and colleagues, who concluded partial cybercrime awareness status on the ground that Internet users were more aware of computer-focused categories of cybercrime than a computer-assisted category (2020).

On the other hand, the finding is consistent with the findings of Hansen (2007). Researchers have concluded that there is indeed a poor and low level of cybercrime awareness, just as the efforts towards increasing it are very challenging (Leukfeldt et al., 2013; Malby et al., 2013; Sasse et al., 2001).

Sequel to the above, awareness of cybercrime could be delineated into three broad categories: (1) adequate awareness- describing a proper knowledge of online criminal activities cum attendant risk factors; (2) superficial or shallow cybercrime awareness- describing awareness of cybercrime that is partial, only limited to those cybercrimes users experienced which is largely inadequate mainly in protecting users against risk behavior exposure and cybercrime victimization; and (3) zero awareness of cybercrime- describing users majorly of lower socioeconomic status (SES) category who know very little or nothing about online criminal activities.

Another objective of the study was to examine categories of cybercrime awareness. The result shows that while most Internet users demonstrated the awareness of fraud-related cybercrime categories (39%), e-theft (15%), hacking (12%), and ATM theft (10%); they were rarely aware of sexually related offenses, cyber-terrorism, malware attacks, spam emails, identity theft, BEC, and Online facilitated money ritual categories as their proportion hovered around 8% and below.

Another objective was to discover the mean difference in participants' awareness of computer-focused and computer-assisted cybercrime categories. It was therefore revealed that Internet users significantly demonstrated more awareness of computer-assisted (M = 2.5; SD = 1.7) than that of computer-focused cybercrime categories (M = 2.2, SD = 1.3), t(1103) = 2.9, p=.000, r =.2. More participants are likely to be abreast of computer-assisted cybercrime categories like e-fraud and e-theft than computer-focused categories like spam and virus attacks. In revealing the possibility of this, a participant from the IDI section (Participant No. 11) put it thus: "yes, I know of online duping because I recently fell victim to that."

In the same token, a similar objective on discovering the significant difference in participants' awareness of violent and property cybercrime categories reveals that Internet users significantly demonstrated more awareness of property cybercrime (M = 2.54; SD = 1.6) than that of violent cybercrime categories (M = 1.82, SD = 1.2), t(1103) = 5.94, p=.000, r =.3. More participants are likely to be abreast of property than violent cybercrime categories. The qualitative data had the same pattern: most of the participants in the IDI section demonstrated more awareness of property cybercrime categories like identity theft, hacking, and business email compromise than they demonstrated the awareness of the violent category like cyber-pornography, online bullying, blackmail, and online facilitated money ritual.

Our results were similar to the findings of Nzeakor and colleagues in that individuals were more aware of computer-focused categories of cybercrime than a computer-assisted category (2020). As argued above, the finding has again reinforced our suspicion that information security awareness is very superficial and insufficient in Nigeria.

Objective 3(a) examined the overall difference in the mean victimization scores of participants who demonstrated cybercrime awareness and those who did not. It was found that cybercrime awareness is positively correlated to cybercrime victimization experiences. On the average, participants who demonstrated more awareness of cybercrime experienced significantly more cybercrime victimization (M = 1.66; SD = 1.7) than those who did not demonstrate awareness of cybercrime (M = .73, SD = 1.4), t(1103) = 7.55, p=.000, r =.52.

A similar objective reveals that of 755 participants who demonstrated awareness of cybercrime, as high as 7 in 10 (N=529; 70%) demonstrated awareness of computer-assisted, while as low as 3 in 10 demonstrated awareness of computer-focused (N = 226; 30%). Meanwhile, of the 226 who demonstrated the awareness of computer-focused cybercrime categories, 89% experienced victimization, as against just 11% that did not experience victimization. On the other hand, of 529 who demonstrated awareness of computer-assisted cybercrime, almost all (96%) experienced cybercrime victimization. More of those who demonstrated computer-assisted awareness appear to experience victimization than those who demonstrated awareness of computer-focused categories of cybercrime.

In the same vein, the objective 3(c), which investigated the correlation between participants' victimization experiences and their awareness of the property and violent cybercrime categories, shows that of 755 participants who demonstrated awareness of cybercrime, as high as 8 in 10 (81%) demonstrated awareness of property cybercrime categories. In contrast, as low as 3 in 10 (19%) demonstrated awareness of violent cybercrime categories. Meanwhile, of the 199 who demonstrated the awareness of violent cybercrime categories, 87% experienced victimization, as against just 13% who did not experience victimization.

On the other hand, of 556 who demonstrated awareness of property cybercrime, almost all (94%) experienced cybercrime victimization, as against just 6% who did not experience victimization. Therefore, more of those who demonstrated property cybercrime awareness appear to experience victimization than those who demonstrated awareness of violent cybercrime categories.

Using the Chi-square test, a further attempt was made to verify whether the relationships between awareness categories and cybercrime victimization experiences were statistically significant. Therefore, it was found that there is a statistically significant relationship between the pattern of cybercrime awareness and cybercrime victimization. In this regard, Internet users who demonstrated more awareness of computer-assisted cybercrime tend to experience more cybercrime victimization than those who demonstrated more awareness of computer-focused cybercrime categories, $X2(1) = 14.50$, $p= .000$. Again, Internet users who demonstrated more awareness of property cybercrime categories tend to experience more cybercrime victimization than those who demonstrated more awareness of violent cybercrime categories, $X2(1) = 12.00$, $p= .001$.

Our results seem to contradict and fine-tune several related studies (Gercke, 2012; Nzeakor, 2016; Kazeem, 2019; Malby et al., 2013; Boateng et al., 2011; Leukfeldt et al., 2013; Nzeakor, 2016). In this respect, it could imply that individuals who have experienced specific cybercrime victimization are more aware of such categories experienced than other categories yet to be experienced. It is also possible that their cybercrime victimization experiences preceded their awareness: they were not aware prior to their victimization experiences. The IDI data also sustained the pattern. For instance, all the interviewed participants admitted being aware of cybercrime even though they all experienced cybercrime victimization.

This position was further confirmed by the quantitative data. For instance, the quantitative data revealed that most participants demonstrated inadequate awareness status; just as they were quick to mention those categories of cybercrime, they experienced as same they were aware of. The result from the IDI sections equally confirmed the results. For instance, Participant No.5, a victim of sexting, was quick to mention the same category of cybercrime they were aware of prior to probing their victimization experiences. Another participant equally revealed she was aware of online account hacking prior to in-depth probing of her victimization experiences. It was revealed that the awareness status of most people was consequent upon their cybercrime victimization experience. Their victimization experiences appear to have preceded their awareness of cybercrime, meaning they were not aware of cybercrime prior to their victimization. In this sense, their awareness status was both concomitant to and limited to the categories of cybercrime victimization experienced.

Conclusion

From the discussion above, it can be concluded that cybercrime is still primarily a crime of ignorance except in some extreme cases of personal idiosyncrasies, offline perpetrated cybercrime, partial awareness, and inherent weaknesses of the Internet facility. The subsisting contradictions in the literature regarding the volume, content, and potentiality of awareness reducing cyber security vulnerability are primarily related to the lack of understanding of the forms and pattern of awareness: adequate, partial, and naïve awareness. In this regard, while naïve and partial awareness is more likely to undermine the cyber-policing role of information security awareness, adequate awareness is more likely to reduce cyber security vulnerability. We, therefore, conclude that although the awareness level appeared to be high in Abia State, Nigeria, there

is enough evidence to believe that such awareness status is not only frail but insufficient, justifying the result of the statistically significant positive relationship between awareness and victimization experiences.

Our findings are consistent with previous research and help fine-tune the literature (Gercke, 2012; Kazeem, 2019; Malby et al., 2013; Boateng et al., 2011; Leukfeldt et al., 2013). Gercke concluded that "certain cybercrimes – especially those related to fraud, such as 'phishing" and "spoofing' – do not generally depend on a lack of technical protection but rather on a lack of awareness on the part of the victims (2012, p. 105). However, the category Gercke referred to should be "adequate awareness" (2012). According to Kazeem, the unsealed indictment shows the evolving tactics of online fraudsters, which has seen them continue to dupe unwitting victims (those who do not have adequate awareness of the scourge) despite numerous awareness campaigns about the online scams (2019). In the words of Malby and colleagues, individual cybercrime victimization rates are higher in countries with lower levels of development (2013). Boateng and colleagues also reported that most cybercrimes go unreported (probably due to lack of awareness on the side of victims) (2011). In addition, Leukfeldt and colleagues opined that the first problem in detecting and investigating cybercrime lies in the fact that victims of cybercrime do not always notice (or do not possess adequate awareness) that they are being victimized (2013). The first bottleneck in the fight against cybercrime is that many cybercrimes will never enter or leave the criminal justice system due to a lack of knowledge of (adequate) cybercrime. Hansen further concluded that with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, most people are still vulnerable to the frailties of human behavior (2007). Fadilpasic instead cautioned that without greater awareness and an increased effort to implement necessary security controls, more attacks would be using an ever-expanding range of technologies and strategies (2019). In the same token, Wall concluded that because the potentiality for our data to be used maliciously is much greater now than ever, it, therefore, becomes increasingly vital that we study the impacts of the Internet, especially as the freedom it brings comes at the cost of the new risks we experience (2010). Just as Malby and colleagues cautioned that it would take a while for public awareness campaigns to build public trust, most users' education or cybercrime campaigns did not necessarily translate into "feeling informed" (2013).

The findings help put other studies like Nzeakor, who found conflicting results with qualitative and quantitative data (2016). The study concluded from quantitative data that cybercrime awareness predicted cybercrime victimization in Imo State. However, it contradicted the finding from the qualitative data, which held that most informants admitted experiencing cybercrime victimization notwithstanding being aware of cybercrime in a better perspective. Therefore, the findings of the current work have helped to put the result of Nzeakor's qualitative data in proper perspective (2016). The high proportion of partial and weak awareness of cybercrime amongst Internet users puts a clog in the wheel of cyber-policing. The finding of the perception study supports the fact that Internet users who are not aware of cybercrime are more likely to experience cybercrime victimization than those who are unwittingly about it. All things being equal, awareness can only serve as an effective cyber-policing strategy when such awareness is adequate.

Another twist to this widespread shallow or lack of awareness status among the populace is that most people do not even know that cybercrime could also occur via an offline medium where ICT gadgets are lost or compromised. For instance, one of the key informants interviewed, a banker, was sure she was free from cyber-attacks because she guarded her digital information.

Nevertheless she lost her laptops in the past, aligning with Wall's findings that everyone is affected at some

point (2010). Because of this reality, the potential for our data to be used maliciously is much greater. It becomes increasingly important that we study the impacts of the Internet, especially as the freedom it brings comes at the cost of the new risks we experience.

Contribution to Knowledge

This study aims to understand better the current trend in cybercrime or information security awareness and the relationship such trend has with cybercrime vulnerability or victimization. Having discovered that most Internet users' awareness status in Nigeria is weak, partial, and insufficient, warranting their increasing vulnerability to cyber-security incidents, we believe that interventions can now be implemented to increase the campaign of adequate awareness, leading to the overall reduction in the spate of cyber security vulnerability. It has also helped strengthen and put other relevant studies in proper perspective.

Relationship of findings to the theoretical framework: The study's findings confirm the RAT of Cohen and Felson (1979) and Victim Precipitation Theory of Wolfgang (1958). Relevance of RAT to the study is captured in explaining the reason for widespread cybercrime victimization in the population, as captured by the test of hypothesis, which shows a significant positive correlation between cybercrime awareness and victimization. In this regard, RAT helps understand the possible link between lack or inadequate guardianship (lack of adequate awareness) and cybercrime victimization. On the other hand, Victim Precipitation Theory (VPT) guided the study in understanding the possible contributions of the victims (where victims lack adequate awareness of cybercrime) towards their victimization.

Recommendations

A robust campaign of information security is strongly recommended. For such information security to be sufficient, it is recommended to be born out of a careful understanding of the frail information system knowledge. It should be carefully designed to educate the general public on the intricacies of information systems. Such knowledge should not be obtained through trial and error or experience. For the awareness to be effective, it should be disseminated via social media- targeting the young people, the illiterates, and females; and through video games and kiddies programs- targeting the children.

References

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Information Technology & People.*

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology 3*(3), 176-183. https://doi.org/10.4304/jait.3.3.176-183.

Amankwa, E., Loock, M., & Kritzinger E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014) (pp. 248–252). IEEE.

Ashaolu, D. (2011). *Combating cybercrimes in Nigeria.* Ibadan: Lifegate Publishers.

Aurigemma, S., Panko R. R. (2012). A composite framework for behavioral compliance with information security policies. In: System Science (HICSS) 45th Hawaii International Conference on System Sciences. Maui, HI: 2012. p. 3248–57.

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

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

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Sociological Review* (44): 588–608.

Fadilpasic, S. (2019). Cybercrime costing businesses millions every minute. Retrieved from https://informationsecurity.report.

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

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2,* 13-20.

Hadlington, L., Binder J., & Stanulewicz, N. (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. Cyberpsychology, Behavior, and Social Networking. Ahead of printhttp://doi.org/10.1089/cyber.2019.0703.

Hansen, J. R. (2007). Cybercrime prevention. In C. B. R. J. K. O'Shea, J. Steete, J. R. Hansen & & T. Ralgh (Eds.), Cybercrime investigations: *Bridging the gaps between security Professionals,law enforcements-and prosecutors* (pp. 261–283). New York: SynGressPublishing.

Internet Crime Complaint Centre (2010). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Internet Crime Complaint Centre (2016). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Internet Crime Complaint Centre (2018). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Internet Crime Complaint Centre (2019). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Israel, G. D. (1992). *Sampling: The Evidence Of Extension Program Impact.* Program Evaluation and Organizational Development, IFAS, University of Florida. PEOD-6.

Joinson, A. N., Reips, U., Buchanan, T., & Paine Schofield, C. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1).

Kazeem, Y. (2019). The FBI's Nigerian email scam ring bust shows how the billion-dollar global fraud has evolved.

Kritzinger, E, & von Solms, S.H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Lee, H. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology,12*(1).

Leukfeldt, R., Sander, V., & Wout, S. (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 cybercrimes? Retrieved from http://www.dallasnews.com

Malby, S., Mace Robyn M., Anika, H., Cameron, B., Stefan, K., & Eva, I. (2013). Comprehensive Study on Cybercrime. *United Nations Office on Drugs and Crime, February*, 1–320. https://doi.org/10.1103/PhysRevLett.105.018904

Mbachu, G. N., & Nazeef, B. (2017, September 30). Cybercrime: Nigeria losing battle against unrelenting-enemies. Retrieved from https://leadership.ng/2017/09/30/cybercrime-nigerias-losing-battle-unrelenting-enemies/

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

Mylonas, A., Kastania, K., & GritZalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platform. *Computer & Security, 34.*

Ndubueze, P. N. (Ed.). (2017). *Cyber criminology and technology-assisted crime control: A reader.* Kaduna, Nigeria: Ahmadu Bello University Press Limited.

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

Nzeakor, O, F., Nwokeoma B. N., & Ezeh, P.-J. (2020). 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.

Ogutcu, G., Te Ozlem, M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. *Computer & Security, 56.*

Rich, W. (2010). Seniors and cyber space. In T. Finnie, T. Petee, & J. Jarvis (Eds), *Future challenges of cybercrime* (pp. 59-60). Virginia: Futures Working Group.

Sasse, M. S., Brosoff, D., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer Interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Siponen, M. T., & Oinas-Kukkonen, Harri (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 60.

Stanton, J. M., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133.

Tsohou, A., Spyros, K., Maria, K., & Evangelos, K. (2008). *Investigating Information Security Awareness: Research and Practice Gaps. Information Security.*

Utcu, G. O., & Testik, O. M. (2015). Analysis of personal information security behavior and awareness. *Journal of Computers & Security*. Retrieved from: www.sciencedirect.com.

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

Wolfgang, M. (1958). *Patterns in Criminal Homicide. European Journal of Criminology, 2*(4), 407-427.

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.

Zhang, J., Reithel, B. J., Li H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

Appendix I:
QUESTIONNAIRE

Letter to Respondents

Dear Respondent,
REQUEST FOR COMPLETION OF QUESTIONNAIRE ITEMS

I am a doctoral student of the above-mentioned Department, conducting a research on cybercrime victimization. You have been selected as one of the respondents in this research. As a user of Information Communication Technology (ICT) devices, you have experience(s) that may be relevant to the objectives of this research. You are therefore kindly requested to answer the questions below as frankly as you can by circling the appropriate box below. Your identity is not required; the information you will give will be treated with utmost confidentiality and used purely for academic purposes.
Thank you for your cooperation.
Yours Faithfully,

Nzeakor, Favour O.

INSTRUCTION: Please circle the appropriate answer like this "O"

SECTION A: SOCIO-DEMOGRAPHY DATA

Please indicate as appropriate, your:

(1) Marital Status:

a. Married
b. Single
c. Widowed
d. Separated

(2) Age (as at last birthday):

a. 20-29
b. 30-39
c. 40-49
d. 50-59
e. 60-70

(3) Religious Affiliation:

a. Christianity
b. Islam
c. Others (please, say).....

(4) Highest Education Level Completed:

a. No formal Education
b. FSLC
c. SSCE/NECO/NABTEB
d. NCE/OND
e. HND/Degree
f. Post-graduate Degrees

(5) Gender:

a. Male
b. Female

(6) Occupation:

a. Student
b. Working Class/Employed
c. Self-employed
d. Unemployed

(7) 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).....

(8) 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).....

(9) What are the internet/ICT enabled devices you own/operate (circle all that applies)?

a. Phone
b. Computer/Labtop
c. IPod
d. Others (please, say).....

(10) You accessed the Internet facilities via which of the following service providers?

a. Through MTN data services
b. Through Glo data services
c. Through Etisalat data services
d. Through Airtel data services
e. Any of the above
f. Other Public cybercafé services
g. Others (please, say).....

(11) What are the online accounts do you operate (circle all that apply)?

a. Facebook
b. WhatsApp
c. Twitter
d. LinkedIn
e. Internet banking
f. Email
h. Instagram
g. Others (please, say).....

(12) Which of the accounts above do you visit mostly?

(13) Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM?

a. Yes
b. No

(14) If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years

(15) Which of the following experience(s) have you had in the last 3 years? (please circle all that apply).

a. My online account(s) (E.g. email, Facebook, Twitter, Instagram, or bank mobile App) has been hacked.
b. I have complied with strange email or call asking me to disclose my personal information, like password, or BVN.
c. I have lost money to stranger I met online, or through phone/email.
d. I have opened/replied spam mail(s).
e. I have received email/text/call that threatened/insulted me.
f. I have visited a stranger I met online and had an ugly experience.
g. My computer/phone has been attacked by malware/virus
h. I have been contacted by criminal gangs to join them
i. My computer/phone/ICT gadget(s) has been stolen/damaged
j. I have been contacted for sexual related activities

(16) If you ticked any of the items in No.15 above, please through which medium did you have such experience(s)? (Please circle all that apply).

a. ATM
b. Online banking
c. Phone
d. Social media (E.g., Facebook, WhatsApp, Instagram, twitter, etc.)
e. Email
f. Websites
g. Others (please, say).....

(17) Which of the followings have you ever done in the last 3 years (please circle all that apply)?

a. I have disclosed my access code/password/PIN to my friend/colleague/relation.
b. I have utilized the same password/access code across multiple online services or applications.
c. I have shared ICT gadgets with a friend/colleague/relation.
d. I have lost/sold/dashed my computer/laptop after usage.
e. Others (please, say).....

(18) If you ticked any of the questions in items No. 15 & 17, could you please say how many times it/they happened in the last 3 years?

a. About once
b. Twice
c. Three times
d. Four times
e. Five times or more
f. Cannot remember

(19) Could you say how much, or what you lost?

a. Phone
b. Laptop
c. Money
d. Car
e. Recharge Card
f. My precious Time/Peace of mind

(20) Was the criminal related/connected/known to you?

a. Yes
b. No

(21) If you have had any of the experiences as described in question No.15& 17 above, did you or anyone else report the incident to the police?

a. Yes
b. No

(22) If yes, please state your experience with the police or any other agency:

(23) If yes, how satisfied were you with the way the police handled the matter?

a. Very satisfied
b. Satisfied
c. Dissatisfied
d. Very dissatisfied
e. Can't say/neither

(24) If you didn't report to the police, could you please state why you didn't report the case to the police? (Please circle all that apply).

a. Not serious enough / no loss
b. Inappropriate for police / police not necessary
c. Police could do nothing / lack of proof
d. Police won't do anything about it
e. Fear / dislike of the police / didn't want involvement with police
f. Reported to other authorities instead
g. Solved it myself / my family resolved it / perpetrator known to me
h. Fear of reprisals
i. I posted it on the social media
j. Others (please, say).....

(25) If you didn't report the case to the police, could you please state how you were able to resolve it?

a. I prayed about it
b. I decided to forget about it
c. I took precautions against its reoccurrence
d. Others (please, say).....

(26) What precaution(s) did you take in order to ensure that you weren't attacked or duped again online? (Please circle all that apply).

a. I did nothing
b. I deleted my online accounts (like Facebook, email, or bank mobile app)
c. I stopped using ATM
d. I don't pick calls from unknown numbers
e. I don't accept friendship request from strangers
f. I installed anti-malware/virus
g. Others (please, say).....

(27) Which of the following factors do you think could be responsible for your online criminal attack(s) [please circle all that apply]?

a. Not being protected with anti-malware/virus
b. Greed/love for money
c. Constantly being online
d. Not being aware of criminal activities online
e. Porosity/weakness of the Internet
f. Ignorance of the online criminals' tricks
g. Carelessness

**Kindly drop your contact if you wouldn't mind a further discussion of your experience(s) with the researcher

Appendix II: QUESTIONNAIRE

1	Are you aware that people have been attacked, raped, lost money or lives through the Internet, phone, or ATM?	Record the responses, and probe to ensure exhaustive discussion.	
2	Ask informant if he/she has been a victim of any of the internet/ ICT crime related activities in the last 3 years?	Probe and record	
3	Ask him/her to please mention the media through which he had such experience(s)	Record	
4	Ask if any of his/her ICT gadgets (E.g., Phone, storage systems, laptop, IPod, etc.,) been consciously or criminally damaged, stolen, or hacked into in the last three years?	Record, and probe for details.	
5	Ask if he/she has had any cybercrime victimization experience(s), like opening spam email or in the last 3 years?	Record, and probe for details.	
6	Ask if she/he has been exposed to any of the risk factors to cybercrime victimization, like disclosing of access code to friends/ colleagues/relations, or transferring money to online impostor, in the last 3 years?	Probe, and record all that apply.	
7	Ask him/her to please say how many times he/she has been victimized online in the last 3 years?	Probe, and record	
8	Ask him/her to estimate how much, or what was lost to the online victimization.	Record	
9	Ask if the criminal was related/connected/known to her/him.	Record	
10	Ask if the incident was reported to the police or any other place?	Record	
11	If yes, ask him to narrate his/her experience with the police.	Record	
12	If he/she didn't report to the police, ask the reason(s).	Probe, and record all that apply.	
13	Ask what other actions he/she took to prevent the reoccurrence; and what he/she did after the incident (since he/she didn't report to the police)	Record	
14	Ask him/her the factors that could be responsible for his/her online victimization?	Record any of, or all that apply.	

Appendix III:
STRUCTURED INTERVIEW FOR THE POLICE OFFICERS

Letter to AIG, Zon 9, Umuahaia

Department of Sociology/Anthropology

University of Nigeria, Nsukka
Enugu State, Nigeria.
September, 2019.

Dear Sir

APPEAL TO BE ALLOWED TO INTERVIEW YOUR RELEVANT OFFICERS

I am a doctoral student of the above-mentioned Department, conducting a research on cybercrime victimization. Some of the professional experiences and records of some of officers and men are considered relevance in realizing some of the objective of this research work. You are therefore kindly requested to grant me the permission to interview some of them for the purpose executing this research. It is also important to point out that their identities are not required. The information they will provide will be treated with utmost confidentiality and used purely for academic purposes.
Thank you for your cooperation.
Yours Faithfully,

Nzeakor, Favour O.

SECTION A: SOCIO-DEMOGRAPHY DATA

(1) Marital Stauts:
(2) Age Bracket
(3) Religious Affliation
(4) Highest Education Level Completed
(5) Gender
(6) Please say your rank
(7) Please say your station

SECTION B: CYBERCRIME VICTIIZATION EXPERIENCES

(8) Has anyone reported any incident/case of having been attacked, raped, lost money or life through the Internet/social media/phone/ATM (probe)?
(9) How often did the report(s) came in the last 12 months (say like once, twice, three times or more)?
(10) What item(s) was reported lost (e.g., phone, rape, money)?
(11) Were the reporters/victims often females or males?
(12) Were the reporters/victims often Younger or older?
(13) Were the offenders often arrested(details, please)?
(14) Were the offenders often related to the victims?
(15) Were the offenders often females or males?

(16) Which medium did the reported online victimization often occur (probe to know whether via Phone, social media, Email, Mobile banking, ATM, others
(17) In comparison with ordinary/conventional crimes (like theft/robbery/rape/battery/etc.) would say people report cybercrime less?
(18) What could you say are the possible reason(s) responsible for the unwillingness of victims to report their cybercrime victimizations/attacks?

Acknowledgments

We acknowledge the exceptional technical assistance from Mr. Francis Okwara in terms of statistical analysis. We also acknowledge the valuable contribution of Dr. Nneka Omego towards expanding the scope of the study.

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

Funding

This work received no funding from any agency.