International Journal of Public Administration and Management Research (IJPAMR), Vol. 6, No. 4, June, 2021. Available online at http://journals.rcmss.com/index.php/ijpamr; www.academix.ng
ISSN: 2350-2231(E) ISSN: 2346-7215 (P)
Akam Simon Sampson & Ojen, Ignatius Mbeh , 2021, 6(4):29-35

Perception Analysis of Covid-19 Pandemic, Cybercrime and Well-Being of Online Fraud Victims in Calabar, Nigeria

Akam Simon Sampson[1] & Ojen, Ignatius Mbeh [2],
Department of Sociology,
Faculty of Social Sciences,
University of Calabar, Calabar, Nigeria
Email: ignetiusojen@gmail.com+2348068137506

Abstract
The study examines the relationship between Covid-19 pandemic, increase in cybercrime and well-being of online fraud victims in Calabar, Cross River state, Nigeria. Specifically, the study (i) examines the most prevalent cybercrime experienced by individuals during Covid-19 outbreak (ii) examine the most vulnerable group of people to cybercrime (iii) examine vulnerability factors (iv) determine the consequences of cybercrime on the well-being of victims in Calabar, Cross River state, Nigeria. The study is descriptive in nature and adopts the mixed methods of data collection. Using qualitative and quantitative research approaches, a sample of 622respondents is drawn from Calabar, the capital of Cross River State, Nigeria. The study adopts multi-stage sampling technique, which consist of purposive, simple random and stratified random sampling techniques to reach the respondents. Findings from the study reveals that during Covid-19 outbreak there is an increase in cybercrime as a result of increased reliance on the internet for social interaction. It is observed that phishing and hacking are among the two prominent types of cybercrime used in attacking victims in Calabar, Cross River State, Nigeria. The study recommends that issues of cyber security should be taking seriously by government and other stakeholders in the communication industry.
Keywords*: Covid-19, cybercrime, fraud, online, victims and well-being*

DOI: URL:https://doi.org/10.36758/ijpamr/v6n4.2021/03

Introduction

The COVID-19 pandemic has drastically and extensively altered life (Hawdon, Parti, & Dearden, 2020). This global pandemic has forced organisations and individuals to embrace new practices such as social distancing, hand washing, wearing of face mask and remote working. Governments are reconsidering ways to ensure that their countries are stable by developing and enforcing new economic plans. (Kawohl & Nordt 2020; Lianos 2020). The fallout of the pandemic is having profound impacts on society and the economy, and it is also influencing and shaping organised criminal activities. Even though some have argued that at these stages of the pandemic, it may be difficult to fully understand, appropriate and to determine the far-reaching impact of the pandemic. What seems clear, however, is that the pandemic has reduced some organized-criminal activities while simultaneously providing opportunities for new ones, and these changes in the organized-criminal economy could have long-term consequences (Global initiative, 2020).Nevertheless, while the world is focused on the health and economic threats posed by COVID-19, cyber criminals around the world undoubtedly are capitalizing on this crisis. Miró-Llinares and Moneva (2019) observe that as persons spend more time connected to the Internet, and less time on the streets, opportunities for street violent and property crimes decrease while Internet crimes increase.

Cybercrime constitutes any and all criminal activities carried out by means of computers or the Internet. While it has been around for quite some time, cybercrime continues to grow in scope and sophistication. Studies (Yitzhak, 2020; Shayegh & Malpede, 2020) have shown that at the pike of the pandemic there was a spike in phishing attacks, hacking, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers. Not only are businesses being targeted, end-users who

download COVID-19 related applications are also being tricked into downloading ransomware disguised as legitimate applications (Matthewman & Huppatz, 2020). As situation that resulted to financial loss, emotional and psychological trauma for most of the victims of Covid-19 induced cyberattack (Cross 2018).The paper provided perception analysis of Covid-19 pandemic, cybercrime and its effect on the well-being of online fraud victims in Calabar, Cross River state, Nigeria. This paper expatiates on the following specific objectives: (i) examines the most prevalent cybercrime experienced by individuals during Covid-19 outbreak (ii) examine the most vulnerable group of people to cybercrime (iii) examine vulnerability factors (iv) determine the consequences of cybercrime on the well-being of victims in Calabar, Cross River state, Nigeria.

Materials and Methods

Research design and study population

This study adopts a cross-sectional survey design, which involves the observations of a sample, or a cross section of a population or phenomenon which is made at one point in time (Babbie, 2010). The study solicits, gathers and analyzes the perception of respondnets on Covid-19 pandemic, cybercrime and well-being of online fraud victims in Calabar, Cross River State, Nigeria. The study area is Calabar, Cross River State, Nigeria. Calabar, the capital of Cross River State is located in South-South, Nigeria. Calabar is divided into Calabar South and Calabar Municipality Local Government Areas and covers an area of about 1,480 Sq km. Calabar is located between longitudes 8^0 17'00 E and 8^0 20'00''E latitudes 4^0 50'00''N and 5^0 10'00''N (Udoimuk, Osang, Ettah, Ushie, Egor, & Alozie, 2014). Calabar is sandwiched between the Great Kwa River to the East and the Calabar River to the West. Calabar falls within tropical equatorial climate with high temperature, high relative humidity and abundant annual rainfall. Two major air masses affect the climate of Calabar as well as other contiguous locations in the West African region. Calabar lies within a tropical region with well-marked rainy and dry seasons. The wet season starts from May and spans to October while the dry season starts from November to April (Ekiji, Nwosu & Agba, 2011).

The three dominant ethnic settlement in Calabar are the Efiks, Quas and Efuts (Effiong-Fuller, 1996); but because of migration occasioned by socio-economic activities, Calabar is today a cosmopolitan society with mixed bag of people from different cultural backgrounds. Calabar owns a seaport, an airport, a market for agro-produce from the hinterlands and home of many industrial outlets. The topography of the study area is the low lying coastal plain of the Calabar River and Great Kwa River. It is relatively undulating with a few hills and valleys running east-west wards. Several rivers/streams exist in the area and are basically drained by the aforementioned rivers. The geography of the area is mainly sand stone. Calabar has a saw-mill, rubber, food, and oil-palm-processing plants; and a cement factory. Calabar has long been an educational centre. Its first church and school, established by the Rev. Hope Waddell of the Free Church of Scotland in 1846, helped influence the Ekpe secret society to pass a law (1850) prohibiting human sacrifice. The city is a home to the prestigious University of Calabar established in 1975, a college of technology, a teacher-training college, and numerous secondary schools. Historically, Calabar was a centre for trade between Europeans on the coast and Africans farther inland. Fish, cassava, bananas, palm oil, and palm kernels were traded at Calabar for European manufactured goods, and the town also served as a major slave-trading depot.

Sample size and sampling technique

The sample size is determined by using the Yamane (1967) formula:

$n = \frac{N}{1+N(e)2}$ Where; n = sample size, N = target population of study, e = error limit $(0.04)^2$ or 0.0016, and 1 = constant. Applying the formula, we have:

$$n = \frac{158674}{1 + 158674\ (0.0016)}$$

$$n = \frac{158674}{1 + 253.8784}$$

$$n = \frac{158674}{254.8784}$$

$$n = 622.54785$$

$$n = 622$$

A sample size of 622 respondnets were selected as the sample size for questionnaire distribution.Respondnets were selected using the multi-stage sampling technique which involves the selection of community clusters, groups, streets, villages, housing units out of which research participants were selected. Both simple random and purposive sampling teachiques were appropraitely applied in the selection of streets, villages, housing units and respondents.

Population and instruments for data collection

The target population is 158,674. The target population of the study is made up of both young and old adults from 18 to 45 years who reside in Calaabar. The choice of selecting this set of people was because they were assumed to either have been victims of cybercrime or have knowledege of people that perpetrate cybercrime. The study basically adopts the questionnaire as the main instrument for data collection.

Research ethicsand methods of data analysis

The study observes all known ethical regulations which guide social science research. These include disclosure policy, informed consent, safety protocols, anonymity and confidentiality. The ethical approval for this study is granted by the University of Calabar Teaching Hospital, Calabar, Cross River State, Nigeria.The quantitative data from the questionnaire is coded, computer processed and analyzed using version 20 of the Statistical Package for Social Sciences (SPSS). Descriptive statistics such as percentages and frequency tables is used in presenting the results.

Results and discussion

Of the six hundred and twenty-two (622) copies of the questionnaire distributed, 612 copies of the questionnaire are validly completed and used for analysis. Majority of the 78.3% of the respondents are male while 21.7% of the respondnets are female. 52.0% of the respondents are 45 years and above, 19.9% are within the age bracket of 36 – 44 years. This is followed by those aged 27 – 35 years (17.8%), while, those aged 18 – 26 years are the least (10.3%). This implies that the majority of the respondents sampled are matured (45 years and above). The distribution of the marital status of the respondents shows that respondents who are married are obviously more than those in other categories and they account for 55.7% of the sample, this is followed by singles (20.4%). Divorced women are 3.3% and those who are separated (2.6%) are the least among the sampled. This finding shows that most of the respondents are married. Data carrying the educational qualification of the respondents reveals that 33.8% of the respondents have completed their tertiary education, 27.1% have obtained their secondary education certificate, while 25.3% have completed their primary education, and 13.7% have no formal education. This finding infers that majority of the respondents are literate enough to make adequate and meaningful contributions to the subject matter of this study.

What is the prevalent cybercrime experienced by individuals during Covid-19 pandemic

The respondnetswere asked to identify the most prevalent cybercrime experienced by individuals during the Covid-19 pandemic. Data in Table 1 reveals that the most prevalent cybercrime experienced by individuals during the Covid-19 pandemic is data modification (31.9%), followed by phishing with 29.4% of respondents. 25.3% of the respondents point out hacking. Furthermore, 24.5% identify the cyber bullying, while, 21.7% mention identity theft. 14.5% of the respondents' support business email compromise, 12.9% of the respondents mention social network fraud, 5.9% speak of cyber vandalism, while, only 1.5% had mentioned cyberstalking. This suggests that majority of the respondents (31.9%) note that the most prevalent cybercrime experienced by individuals during the Covid-19 pandemic.

Table 1: Percentage distribution of respondents on the prevalent cybercrime during Covid-19 pandemic

Prevalent cybercrime	Mentioned	Not mentioned	Total
Data modification	36 (5.9)	576 (94.1)	612 (100.0)
Phishing	133 (21.7)	479 (78.3)	612 (100.0)
Hacking	155 (25.3)	457 (74.7)	612 (100.0)
Cyberbullying	150 (24.5)	462 (75.5)	612 (100.0)
Identity theft	79 (12.9)	533 (87.1)	612 (100.0)
Busniess email compromise	195 (31.9)	417 (68.1)	612 (100.0)
Social network fraud	180 (29.4)	432 (70.6)	612 (100.0)
Cyber vandalism	89 (14.5)	523 (85.5)	612 (100.0)
Cyberstalking	9 (1.5)	603 (98.5)	612 (100.0)

Source: *Fieldwork (2020)*

Group of people vulnerable to cybercrime

The result in Table 2 reveals that a significant percentage of the respondents (75.7%) indicate that the old are the most vulnerable group of people to cybercrime. While only 24.3% reported that the young are the most vulnerable group of people to cybercrime.This finding suggests that a significant number of the respondnets are of the view that old people are more vulnerable to cybercrime.

Table 2: Percentage distribution of the respondents on the vulnerable group of people to cybercrime

Vulnerable age group	Frequency	Percentage (%)
Young	149	75.7
Old	463	24.3
Total	**612**	**100.0**

Source: *Fieldwork (2020)*

Vulnerability factors

In Table 3, the various vulnerability factorsmentioned are lack of computer skills (19.9%), lack of internet skill (29.2%), less awarness programme (29.1%), underreportingof cybercrime (21.7%). This finding implies that majority of the respondents (29.2%)reported lack of internet skill is the reason of vulnerability.

Table 3: Percentage distribution of respondents' vulnerability factors

Vulnerability factors	Mentioned	Not mentioned	Total
Lack of computer skills	122 (19.9)	490 (80.1)	612 (100.0)
Lack of internet skills	179 (29.2)	433 (83.7)	612 (100.0)
Less awariness programme on cyber threats	178 (29.1)	434 (89.7)	612 (100.0)
Underreporting of cybercrime	133 (21.7)	479 (90.0)	612 (100.0)

Consequences of cybercrime on the well-being of victims

Data in table 4 reported that consequences of cybercrime on the well-being of victims reveals that 20.8% of the respondents indicate financial loss as the consequence of cybercrime, 17.3% indicate depression, 15.2% of the respondents said it leads to lower self esteem, 11.3% had other opinions, 7.8% indicate identity theft, 6.7% state that it lead to decrease in the sense of coherence, while, another 6.7% testify that lead to credit cards being opened in the victims name.

Table 4: Percentage distribution of respondents on the consequences of cybercrime on the well-being of victims

Effect	Mentioned	Not mentioned	Total
Depression	106 (17.3)	506 (82.7)	612 (100.0)
Lower self esteem	93 (15.2)	519 (84.8)	612 (100.0)
Decrease in the sense of coherence	98 (6.7)	514 (84.0)	612 (100.0)
Identity theft	48 (7.8)	564 (92.2)	612 (100.0)
Credit cards opened in the victims name	41 (6.7)	571 (93.3)	612 (100.0)
Others	69 (11.3)	543 (88.7)	612 (100.0)
Financial lost	127 (20.8)	485 (79.2)	612 (100.0)

Source: *Fieldwork (2020)*

Test of hypotheses

Hypothesis one

Substantive hypothesis (H_1: Older people are more likely to fall victim of cybercrime than the younger people

Null hypothesis (H_0): Older people are less likely to fall victim of cybercrime than the younger people

Table 5: *Percentage distribution of respondents by*age group *and cybercrime vulnerability*

	Cybercrime vulnerability		Total
Age group	More vulnerable	Less vulnerable vulnerable	
Younger	154(64.4%)	85(35.6%)	94(100.0%)
Older	203(54.4%)	170(45.6%)	373(100.0%)
Total	**357(58.3%)**	**255(41.7%)**	**612(100.0%)**

χ^2= 6.007[a] df=1, p< .014 critical/table value=3.841
Source: *Fieldwork (2020)*

To test hypothesis one, the age group is cross-tabulated with the feelings of the respondents to test the cybercrime vulnerabilty of people. The result presented in Table 5 reveals thus: majority (64.4%) of the respondents are younger people who feel that theyare more vulnerable to cybercrime, while, just 35.6% of those with younger people feel that are less vulnerable to cybercrime. Furthermore, 54.4% of respondents are older people, they indicate that the vulnerability on them is positive, while, slightly below half (45.6%) of the respondents maintained that the vulnerability impact on them is negative. The Chi square test result shows that computed χ^2 is 6.007, while, the critical/table χ^2 value is 3.841 and df = 1. The test shows that there is a statistically significant relationship (P <.014) between age and cybercrime vulnerability. From the decision rule, since the chi-squared calculated (6.007[a]) is greater than the chi-squared tabulated (3.841) we accept the substantive hypothesis, which states that theolder people are more likely to fall victim of cybercrime than the younger people while, the null

hypothesis, which states that the older people are less likely to fall victim of cybercrime than the younger people is rejected.

Hypothesis two

Substantive hypothesis (H_1: Urban dwellers are more likely to fall victims of cybercrime than those in the rural areas

Null hypothesis (H_0): Urban dwellers are less likely to fall victims of cybercrime than those in the rural areas

Table 6: *Place of residence and impact of cybercrime*

	Cyybercrime vulnerability		**Total**
Place of residence	**More vulnerable**	**Less vulnerable**	
Urban area	147(47.9%)	160(52.1%)	307(100.0%)
Rural area	210(68.9%)	95(31.1%)	305(100.0%)
Total	**357(58.3%)**	**255(41.7%)**	**612(100.0%)**

χ^2= 27.680[a] df=1, p< .000 critical/table value=3.841

Source: *Fieldwork (2020)*

To test hypothesis two, place of residence was cross-tabulated with the feelings of the respondents to test the impact cybercrime has on the people. The result displayed in Table 6 showed that 47.9% of respondents who reside in the urban area feel that they are more vulnerable to cybercrime, while majority 52.1% of them feel that they are less vulnerable to cybercrime. Furthermore, 68.9% of the respondents who reside in the rural area feel that they are more vulnerable to cybercrime, while, a few of them (31.1%) assert that they are less vulnerable. To gain clarity on the data presented in the Table 6, given the computed χ^2 =27.680[a]and critical/table χ^2 value of 3.841; df = 1, the test shows that there is a statistically significant relationship (p<=.000) between the place of residence and cybercrime vulnerability. This suggests that one's place of residence determine the extent of the person vulnerability to cybercrime.

Discussion

The study first hypothesis states that older people are more likely to fall victim of cybercrime than the younger people. According to the findings of the study, cyber victimisation cut across all age group, however, the older persons were found to be more vulnerable to cyber victimisation because of their pecularities and preferences.The impact of their victimisation is more severe and dangerious when compare to other age groups. These results are in line with earlier research on Covid-19 and cybercrime victimisation. Results also reinforce previous research submissions on the relationship between onlinevictimisation and well-being of victims. Thus, even though cybercrime victimisation does notshare the spatial and temporal connection between victims and offenders as is typical in offlinecrime it has the potential to be harmful for their victims' well-being.

Furthermore, the result of the second hypothesis shows that urban dwellers are more likely to fall victims of cybercrime than those in the rural areas. The findings of this study are in linewith the risk society hypothesis, one of the dominant theoretical models that buttresses the connection between modernisation and degrading social enviornment. However, while rural dwellers were found to be less likely to suffer cyber victimisation, the study also demonstrated that a handful of rural dwellers have been victims of phishing and hacking. Thus, the findings seem to show thatno one iresspective of the person resident is completely exempted from cybercrime as studies have shown that proportion of attacks between rural and urban dwellers

varies significantly. Earlier studies have extensively discussed the variation in terms of vulnerability of cybercrime between rural and urban dwellers.

Conclusion and recommendations

Just as Covid-19 is having global impact, so too are the action of cybercriminals who are exploiting the current situation with a significant surge of activities worldwide. The study conclude that cybercrime is a massive problem that requires internet users to be watchful and maintain a high level of security consciousness. As new security measures are being developed all the time to keep pace with criminals and giving the surge of cyberattacks reported and detected in the wake of the Covid-19 pandemic, it is important for computer users to use strong and unique passwords, combining letters, numbers, and special characters. Internet users should have an up-to-date Internet security suite for real-time protection against viruses and malware. Also, relevant programs should be updated, this include both security suites and commonly-used programs update constantly as they implement safeguards against new threats. Internet subscribers should avoid downloading and installing programme from unofficial repositories.

References

Cross, C. (2018) '(Mis)understanding the impact of online fraud: implications for victim assistance schemes', Victims & Offenders 13(6): 757–76. doi:10.1080/15564886.2018.1474154. [Taylor & Francis Online], [Web of Science ®], [Google Scholar]

Global initiative (2020). CRIME AND CONTAGION: The impact of a pandemic on organized crime. https://globalinitiative.net/wp-content/uploads/2020/03/GI-TOC-Crime-and-Contagion-The-impact-of-a-pandemic-on-organized-crime-1.pdf

Hawdon, J., Parti, K. & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. American Journal of Criminal Justice (2020) 45:546–562

Kawohl, W. and Nordt, C. (2020) 'COVID-19, unemployment, and suicide', The Lancet Psychiatry 7(5): 389–90. doi:10.1016/S2215-0366(20)30141-3.

Lianos, M. (2020) 'The welfare state: where hope and fear meet', European Societies 22(3): 291–2. doi:10.1080/14616696.2020.1771861. [Taylor & Francis Online]

Matthewman, S. and Huppatz, K. (2020) 'A sociology of Covid-19', Journal of Sociology .

Miró-Llinares, F. and Moneva, A. (2019) 'What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?"', Crime Science 8(2). doi:10.1186/s40163-019-0107-y

Shayegh, S., & Malpede, M. (2020). Staying home saves lives, really! Social Science Research Network Electronic Journal https://doi.org/10.2139/ssrn.3567394.

Yitzhak, Y. (2020). Social media interest is spiking worldwide—Except for Linkedin. The Next Web. (April 2, 2020); https://thenextweb.com/socialmedia/2020/04/02/social-media-interest-spiking-coronavirus-exceptlinkedin/. Accessed 17 Apr 2020.