TAFFD's Journal
ISSN 2643-4938 (online) · ISSN 2769-0490 (print)

OPEN ACCESS

COVID-19 and Cyber Insecurities: Prevalence, Causes and the Way Forward

Chioma Chigozie-Okwum

Published in TAFFD's Journal, Vol. 3, Issue 1, pp. 26–32, 2021
Article page https://journal.taffds.org/articles/covid-19-and-cyber-insecurities-prevalence-causes-and-the-way-forward-1-26

CC BY 4.0 **Licence**

© 2021 The Author(s). Published by Transdisciplinary Agora for Future Discussions Inc. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Licence terms: https://creativecommons.org/licenses/by/4.0/

This page was added by the journal. The article begins on the next page.

COVID 19 and Cyber Insecurities: Prevalence, Causes and the Way Forward

Chioma Chigozie-Okwum
Department of Computer Science, Spiritan University, Nneochi, Nigeria
Email: cyberchioma@gmail.com

ABSTRACT
The global COVID 19 pandemic outbreak spread fear and uncertainties around the globe, but it, however, provided a near-perfect condition for cybercrime, and cybercriminals exploited this vulnerability. Hence, the research became imperative with the increasing cases of cybercrime attacks on digital citizens. The research adopted a cross-sectional survey research approach, where a descriptive study was embarked upon to identify the state of cyber security in Nigeria during the COVID 19 pandemic lockdowns. The study investigated using structured questionnaires administered online via the Google forms platform, the prevalence and patterns of cyber insecurities, and strategies to be adopted in curbing these insecurities. One hundred fifty respondents were sampled, and the study results were analysed using descriptive statistics. The study revealed prevalent nefarious activities by cybercriminals during the study, and these cyber-attacks occurred often. The study further showed that Facebook, WhatsApp and Instagram were the most used platform for these attacks. Ponzi schemes, Phishing attacks, click frauds and hacking of accounts were the most prevalent attacks regimens observed by the study. The cyber-attacks exploited the poor awareness of citizens on basic cyber hygiene best practices, poor dissemination of information by the government and donor agencies, and poor investigation of crimes. The attacks mostly mimicked aid programs by the government, civil societies and donor agencies. The study suggests an increase in user education and awareness and proper investigation and prosecution of cybercrimes as ways of mitigating against these menaces.

KEYWORDS: COVID-19, Cyber Insecurities, Cybercrimes, Impact, Cybersecurity

INTRODUCTION
The world in 2020 experienced a halt orchestrated by a dangerous virus COVID 19 that besieged the globe. It started like a costly joke but culminated into widespread fear, panic and confusion as no one was prepared for what it brought with it. In a twinkle of an eye, streets were vacated, allies became lonely, and the hospitals became overwhelmed with the rising cases of infections as death tolls surged. In such a state of panic and desolation, people scrambled for information on how to stay safe and relief materials to cushion the harsh effects of total lockdowns imposed by the governments. In the face of the increasing fiasco, several agencies, benevolent individuals and even the government started rolling out palliative programs and packages to cushion the effects on citizens. Hospitals overwhelmed began to run out of medical supplies and were searching for suppliers as the whole world was under the same siege.

The widespread fear, uncertainty and quest for survival created a perfect situation for cybercriminals to siege vulnerable people. Cybercriminals usually look for vulnerabilities to exploit, and the situation created by the COVID 19 Pandemic was not any different. Cyberspace became laden with phishing attempts, malicious links, social engineering attacks, to mention a few. When the world was in great panic, cybercriminals saw the perfect situation to unleash on people whose guards were already down due to the ravaging pandemic.

With the COVID 19 pandemic breaking out in late 2019 and spreading across the world in early 2020, lockdowns were imposed as a means of curtailing the spread of the virus. This caused widespread panic among citizens as the lockdown came with pay cuts, job losses and wanton lack. In Nigeria, online users began to experience many cyber-attacks

in the guise of relief and aid towards ameliorating the lockdown effects. Web phishing attempts, Ponzi schemes, social engineering, and click frauds were beginning to become familiar sights. The Nigerian cyberspace began to assume an insecure state as cybercriminals exploited the vulnerability of online users.

In the light of the preceding, a descriptive study was embarked upon to ascertain the state of cyber security in Nigeria at the time, with the aim of the research being to analyse the state of cyber security during the global COVID 19 pandemic with particular reference to the Nigerian state. To achieve the aim, the following specific objectives aided the research;

1. Identification of the state of cyber security during the period of the pandemic.
2. Identification of the cybercrime patterns that were prevalent within the period of the pandemic
3. Identification of measures to curb the spread of cyber insecurities in the face of a global pandemic

REVIEW OF RELATED LITERATURE

Cybersecurity uses policies, hardware, software and people in a multidisciplinary approach to mitigate against the occurrence of cybercrimes and fashion out strategies to recover from and minimise the impact of cybercrimes if they eventually occur. It involves a combination of policies, security protocols, actions, an array of support tools, training regimes, best practices, quality assurance and a total of technologies used to protect the organisation or individual cyber environment and Assets. The Assets protected include all connected devices, human factors, the support infrastructure and the information transmitted. Other valuable assets include Applications, services and the communication channel as well. According to Korff (N.d), cybersecurity works towards attaining the security of the assets of organisations and individuals from threats in a rapidly evolving threat landscape.

The importance of cybersecurity cannot be overemphasised and should be a critical discussion among all levels of government and management. This is because the rapid evolution of the cybercrime attack landscape threatens individual, organisational, national and international security. The need to declare cyber threats as national emergencies is not negotiated.

Cybercriminals have always been profiled to exploit trending issues to wreak havoc on unsuspecting citizens (WHO, 2021). It, however, is not out of place to start experiencing a surging increase in phishing emails and messages and even proliferation of spread of malicious links, to mention but a few. The scams are because humans naturally try to seek solace and succour in the face of crisis, creating a perfect vulnerability for criminals to exploit.

Cybercrime exploit changes in situations, like a change in government policy, the launch of new products, and the outbreak of crises like war, pandemic, or even natural disasters. The fear, uncertainty and poor access to information at these times are the top vulnerabilities exploited. Such times as during the outbreak of Ebola and SARS are examples of similar situations exploited by cybercriminals as they exploit the COVID 19 pandemic. These situations create a perfect opportunity for web phishing attacks, as they craft their emails to mimic relevant authorities. In a state of panic, the vulnerable public may not decipher these illegitimate emails and the propensity to fall victims is very high.

The COVID 19 pandemic, with its resulting imposed physical distancing, led to the proliferation of online activities as schools, churches and work activities moved to cyberspace. According to the Council of Europe (2020), the crisis forced people to rely on digital systems and the internet to work, shop, and disseminate information to reduce the impacts of the imposed physical distancing. This reliance created vulnerabilities that were exploited by malicious cybercriminals to their advantage. Situational crime prevention approaches crime reduction and focuses on situations fuelling crime. Eck and Clark (2019) suggest that situational crime prevention focuses on the criminal acts and their settings and pays less attention to the offender's characteristics. Situational crime prevention does not evaluate the criminal's

tendencies to commit a crime but looks at the enabling environments encouraging the crimes.

The situational crime school of thought proponents submit that criminals take to crime based on the seemingly favourable and available opportunities. They further stated that situational factors could encourage and motivate criminals to commit crimes, and addressing these factors can reduce the crime rates. Situational crime prevention has proven effective in handling trivial, standard and grave crimes. Situational crime prevention approaches crime reduction and focuses on situations fuelling crime. The pandemic period thus provides a suitable situation for cybercrimes and attacks. The surge in cybercrimes with the spread of the pandemic creates an avenue and a perfect situation for cybercriminals to perpetrate crimes. Against this backdrop, it can be stated that if the vulnerabilities orchestrated by the COVID 19 situation are checked, the crimes could be checked.

Weerth (2020) submits an increase in cases of cyberattacks that are bouncing off the COVID 19 pandemic, these attacks target organisations and individuals in such attacks as phishing attacks, ransomware, malware, among others. Criminals try to scam relatives of sick people, hospitals seeking medical supplies and personal protection equipment, and even individuals seeking aids and palliatives from the government and donor agencies. Malicious links to water holing sites abound; the attacks are one too many, and victims keep falling to these attacks.

UNODC (2020) stated that with restrictions to physical congregations and movements, there is a geometric increase in the number of online transactions, with several eCommerce platforms launched. Cybercriminals have also infiltrated the eCommerce landscape with malicious and dangerous platforms. These raise vulnerabilities as cybercriminals leverage search engine optimisation to make these malicious platforms point to the first call. Unsuspecting victims visit these danger zones, and they end up giving away sensitive credentials to cybercriminals.

The Central Bank of Nigeria (2020) opined that cyber-criminals are taking advantage of the current "COVID-19" pandemic to defraud citizens, steal sensitive information, or gain unauthorised access to computers or mobile devices using various techniques. Some of the cyber-criminal activities using the COVID-19 pandemic as outlined include Phishing campaigns in which cyber-criminals send out emails claiming to be from health organisations such as the Nigerian Center for Disease Control (NCDC) or the World Health Organization (WHO). Those emails may contain a link that, if clicked, steals login credentials or other confidential information from the victim's computer or mobile device. Cyber-criminals have also been sending messages via social media or emails asking people to click on links to register to get their COVID-19 relief packages from the government or other organisations. They use this to get confidential information from unwary victims. Relief package scams also come in the form of phone calls asking people to provide their banking details to receive relief packages.

The rate of exploiting the helplessness of citizens with increased uncertainty orchestrated by COVID 19 remains alarming. In an August 2020 report, Interpol submitted that after research lasting four months between January and April 2020, the result showed that about 907,000 spam messages, 737 incidents related to the malware and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners. Distributed denial of service attacks, Phishing, malware infestation and misinformation (fake news) were prevalently plaguing cyberspace with regards to the COVID 19 insurgency. The report, however, predicted that Future primary areas of concern included vulnerabilities caused by increased deployment of remote work, widespread COVID 19 themed phishing emails, especially when a COVID-19 vaccination becomes available, email compromises and finally, a spike in network intrusion and cyberattacks to steal data.

RESEARCH METHODOLOGY

The study adopted a quantitative research methodology in which a field survey was

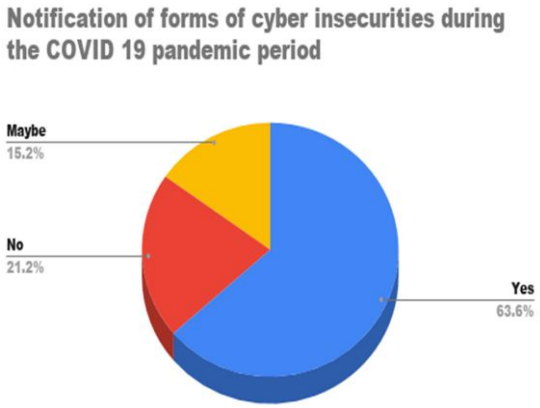
conducted between April and June 2020 to decipher the state of cybersecurity during the period of the COVID 19 pandemic induced lockdown in Nigeria. The research followed a descriptive research methodology where an online survey was carried out—the population of the study comprised about 27 million social media users in Nigeria. However, 150 respondents were purposively sampled, bringing the sample size for the study to 150 participants.

The instrument for data collection was an online questionnaire prepared and distributed using the Google forms platform. The instrument was validated via a pilot study on a group of 10 respondents selected from the Faculty of Natural and Applied Sciences of the Spiritan University, Nneochi, with a rubric to analyse the quality/coherence, clarity, and usefulness of the content of the instrument. Exploratory factorial analysis was used to analyse the instrument's reliability, internal validity, and scale validation. The result of the pilot study validated the instrument as a valuable tool to collect data for the study. Survey responses were analysed using descriptive statistics.

RESULTS AND DISCUSSION

The results from the research are discussed below:

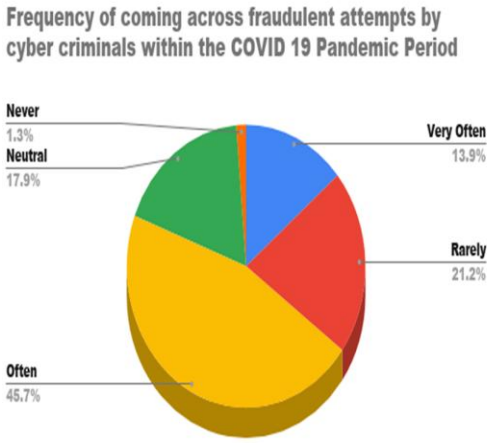
Figure 1: Notification of existence of cyber insecurities



The study, in its attempt to identify if respondents witnessed any form of cyber-criminal activities during the period of the COVID 19 lockdown in Nigeria, discovered via responses provided by the sampled respondents that; 63.6% of the sampled respondents answered in the affirmative that they noticed several attempts made by cybercriminals to defraud people within the period. Furthermore, 21.2% stated they did not notice any form of criminal activities going on, while 15.2% were neutral and indecisive as to if they did notice such activities or not.

The result showed that a good majority of the respondents gave insight into the existence of these nefarious attempts and indicated that cyberspace was grossly unsafe with fraudulent attempts by cybercriminals to exploit the helplessness and vulnerability of the citizens to their advantage.

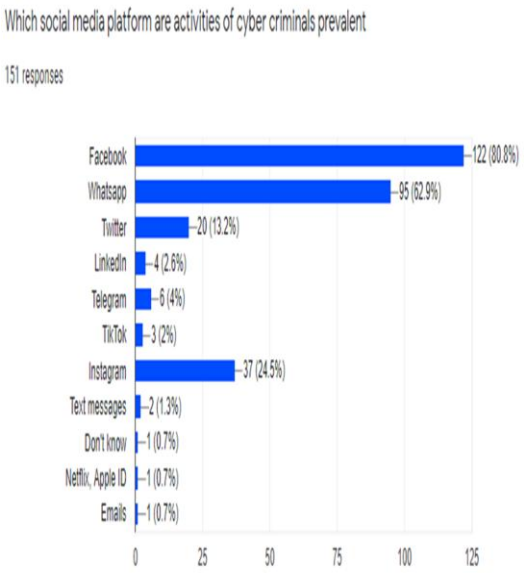
Figure 2: Frequency of Cybercrime attempts



As presented in figure 2 above, the results showed the frequency of these attack attempts; 13.9% of the sampled respondents stated that the attempts were very often, 45. 7% stated they often came across these attempts to defraud them by cybercriminals, 17.9% were neutral and indecisive, and 21.2% stated that the frequency was rare, while 1.3% submitted that they never came across these attempts.

The results provide a very glaring scenario, one which paints a picture of a very persistent attempt by cybercriminals to keep making attempts to exploit the vulnerable victims. As stated earlier, cyber criminals fall into the situational crimes school of thought submissions. They make the best of situations such as an outbreak of a pandemic with its attaining fears, dangers and uncertainties to make unscrupulous attempts to defraud unsuspecting citizens.

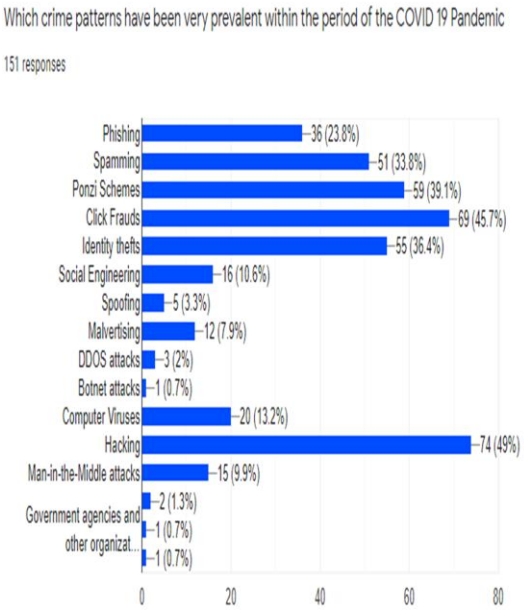
Figure 3: Social Media platform with the most cases of these cyber insecurities



Source: Field Survey 2020.

The study further attempted to identify which of the social media platforms was used mainly by cybercriminals in carrying out their activities during the research period. Research results showed that Facebook was the busiest at the time, with 80.8% of the sampled respondents reporting the rapid hacking of Facebook accounts and subsequently using those accounts to push PONZI schemes and other financial frauds. Other platforms prevalently used were WhatsApp and Instagram. These platforms were used to push fake giveaways and mimic government and other agencies palliative packages. Other platforms like TikTok, Telegram and Instagram did not record much of these activities. Phishing emails and messages were also on the increase, as reported by the respondents.

Figure 4: Most prevalent attack pattern



In the weeks following up to the COVID 19 induced lockdown, we tried to identify the most prevalent cybercrimes witnessed by our respondents during the period and the results as seen in figure 4 above showed that the attacks in order of prevalence include hacking of accounts (49%), Malicious URL click frauds (45.7%), Ponzi Schemes (39.1%), Identity thefts (36.4%), Proliferation of Spam messages (33.8%), Phishing attacks at 23.8% and malware infestation (13.2%). Other crimes identified include social engineering, spoofing, malvertising, DDOS attacks, a man in the middle attacks, among others.

Table 1: Causes of the hike in cyber insecurities during the COVID 19 lockdown in Nigeria.

Response	Frequency	Percentage (%)
Lack of awareness and knowledge of cybercrimes patterns	151	100
The spread of uncertainties with the spread of the COVID 19 pandemic encouraged the growth of cyber insecurities.	120	79.47

Job losses left many people vulnerable in the face of the global COVID 19 pandemic, and hence they became easy targets for cyber-attacks.	**151**	**100**
The citizen's lack of appropriate information is a weakness exploited by the cybercriminals.	**150**	**99.34**
Lack of a skilled workforce to combat cyber insecurities was also a cause for increased cyber insecurities.	**135**	**89.40**
Cybercriminals were mimicking and exploiting several palliative channels rolled out by the government and civil society groups to defraud unsuspecting victims.	**146**	**96.69**
Poor investigation procedures and lack of prosecution of offenders is a propelling factor for the proliferation of cyber insecurities in Nigeria at the time.	**100**	**66.23**

Source: Field Survey 2020

It was deduced from the study that significant causes for the sporadic increase in cyber insecurities at this time could be traced to a lack of awareness by the citizens of what constitutes cybercrimes and the attack regimens. This, therefore, accounts for the reasons why citizens became very vulnerable in the face of uncertainties raised by the global pandemic. Job losses, hunger, uncertainties as to what tomorrow will bring boxed people into a vulnerable spot that became an avenue for cybercriminals to exploit actively. If citizens had some information on these issues, the prevalence would not be so much. Get rich quick scheme, mimics of palliative programs, phishing messages, social engineering and the likes abounded, and people fell for them due to lack of knowledge and appropriate information. The government agencies responsible for national orientation failed to raise the level of awareness.

The law enforcement agencies lack the requisite technical know-how to investigate and prosecute these crimes thoroughly, and offenders are not usually punished optimally to serve as a deterrent to others. To this end, Nigerian cyberspace assumes a near haven state, making it very conducive to the proliferation of these crimes. If criminals are quickly apprehended, prosecuted and punished adequately, the issues surrounding the sporadic increase in cyber insecurities would be minimally controlled.

The study further identified ways of reducing the prevalence of cyber insecurities as suggested by the respondents and these solutions include:

- Citizenship awareness programs on dangers and types of cybercrimes and advocacies for cyber hygiene best practices need to be strengthened.
- The government need to educate the citizens on the correct channels to adopt in applying for and harnessing palliative programs.
- Creation of better technology to help curb cyber insecurities.
- Scrutinising of every information flying round social media.
- To curb cyber insecurities in Nigeria, the offenders have to be appropriately prosecuted once reported to the proper authorities.
- Companies should make sure they are constantly checking whether their staff comply with best practice guidelines concerning two-factor authentication for accessing company networks and webmail.
- Also, encryption on laptops and mobile devices is more convenient for employees working from home to use their devices to work. This makes it easy for data leakage and potential unauthorised access to company files.

- To provide an opportunity for training Nigerian professionals in the area of cyber insecurities that meets international standards.
- Government should strengthen existing laws against cyber security and enforce adequate implementation of those laws.
- Punishment of offenders should be enforced.

CONCLUSION AND RECOMMENDATIONS FOR FUTURE STUDIES.

In the face of growing concerns caused by the sudden outbreak of a global pandemic, perceived and confirmed by this study a surge in the rate of cyber insecurities in Nigeria. This sporadic increase, as was seen, stems from the fact that cybercriminals, like other kinds of criminals' elements, usually exploit vulnerable situations to unleash attacks on vulnerable victims.

The study reported a very high frequency of attack attempts geared towards defrauding victims during the study period, with social media platforms, especially Facebook, WhatsApp and Instagram, playing hosts to the majority of these fraudulent activities. Furthermore, the study identified Ponzi schemes, phishing attacks, click frauds and hacking as the most used cyber-attack patterns during the period. The sudden rise in cyber insecurities the research exposed was because of citizens' uncertainties as orchestrated by the pandemic induced lockdowns. Job losses, closure of businesses and pay cuts forced the citizens to seek alternative income sources online. Cybercriminals exploited this vulnerability coupled with poor information dissemination and hence unleashed attacks on vulnerable victims.

To curb the surge in these cyber insecurities, the study recommends the government and civil societies increase awareness programs on cyber safety hygiene and best practices and disseminate the correct information on how citizens can access aids and palliatives to prevent them from falling victims to scammers. Cybercrimes should be appropriately investigated and prosecuted, and the total weight of the law should be invoked on offenders.

Facebook, WhatsApp and Instagram are exploited more by cybercriminals than more professional platforms like LinkedIn is a good area future research can be the next focus.

REFERENCES

Carsten Weerth, (2020). "INTERPOL on COVID-19: COVID-19 Crime and Fraud Alert Technical Report", April 2020, DOI: 10.13140/RG.2.2.33650.25282.

Central Bank of Nigeria, (2020). "Alert! Beware of COVID-19 Cyber-attacks, Fraud". Central Bank of Nigeria Press Release, April 06, 2020, www.cbn.gov.ng.

Council of Europe (2020). "Cybercrimes and COVID 19". Available @ Douwe Korff, (N.d). https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19

Cyber Security Definitions. Available @ http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Interpol (2020). "INTERPOL report shows alarming rate of cyberattacks during COVID-19". Available @https://www.Interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Shopify registered more than 500 eCommerce sites for COVID or coronavirus in last two months. @https://www.nytimes.com/2020/03/24/business/coronavirus-eCommerce-sites.html

United Nations Office on Drugs and Crime, (2020). UNODC-ROSA's response to COVID-19: The L.E.A. and Cybercrime Segment, April 2020.

World Health Organization, (2021). "Beware of Criminals Pretending to be W.H.O.". Available at www.who.int. Retrieved on April 27 2021.