LAUTECH Journal of Computing and Informatics (LAUJCI) – ISSN: 2714-4194
Volume 2 Issue 1, May 2021 – www.laujci.lautech.edu.ng

Safeguarding Online Payment Systems from Cyber-Attacks during and beyond Covid-19 Pandemic - A Technology Threat Avoidance Approach

Onamade, A.A
Department of Computer Science
Adeleke University,
Ede, Osun State, Nigeria
onamadeakintoye@gmail.com

Sokoya, O.S
Department of Computer Information Sciences
University of the Cumberlands
6178 College Station Drive Williamsburg, KY 40769
daresokoya@gmail.com

Oduwole, O.A.
Department of Computer Science
Adeleke University,
Ede, Osun State, Nigeria
dayooduus@yahoo.com

Adegbite, O
Department of Computer Science
Adeleke University,
Ede, Osun State, Nigeria
sheykole@gmail.com

ABSTRACT

The use of online payment systems witnessed tremendous increase during the COVID-19 lockdown period. Lockdown became necessary and was enforced by the government of most countries of the world, upon the advice of the WHO as an effective method to check the spread of the disease. This left most citizens with online services as the only best alternative. This paper investigates the activities of cybercriminals and its effects on the use of Debit cards and Webpages payment modalities among some undergraduates in Nigeria. Online questionnaire and convenience sampling technique were deployed, to elicit information from universities that shifted onto online payment systems during the period of pandemic. Cronbach Alpha tests and Cross-tabulation with Chi-square were carried out using SPSS version 20 statistical package to analyze 118 valid data collected. Face and content validities of research instrument were done by two experts in the field of cyber-security. Pilot test was done and the corrected version of the questionnaire was administered. Reliability tests on Safeguard measure (0.72), Cyber-Treats (0.95), Impacts of cyber-attacks (0.79) and Challenges with online payments (0.90) showed acceptable Cronbach's Alpha values. Our investigation showed that respondents experienced Spam, Malware, Web-application attacks, Phishing and Identity thefts among other attacks during the lockdowns. We conclude that from a safety perspective, this study emphasizes the use of safeguard measures such as the use of strong passwords, secured webpage, licensed antivirus, keeping the PIN number and password secret by every online user are very crucial to mitigate the activities of cybercriminals.

Key words: Online payments, WHO, COVID-19, cyber-attacks, safeguard

1. INTRODUCTION

Online payment is a common phenomenon these days. Online transactions have been encouraged and still being encouraged by all levels of government in the country because of its numerous advantages (Farringer, 2019). The advantages of online payment include convenience of payment, low cost of tractions, transaction time savings and efficient service delivery among other things. Every business organizations and higher institutions have keyed into its usage. Tuition payments among undergraduates are also largely done through portal systems.

However, there have been number of reported cases of cyber-attacks (Farringer, 2019, Houssain *et al.*, 2019, Daniel *et al.*, 2019) among unsuspecting victims in the society. The educational sector is no exception. As e-commerce technology advanced, it is crucial to broaden the literature related to online payment systems to help educate online users on how to properly prepare for cyber-attacks and mitigate them.

In this research, an empirical study was carried out on the activities of cybercriminals among undergraduates in some institutions in the country i) to identify the categories of cyber-attacks experienced during pandemic ii) to examine the effects cybercriminals activities on the undergraduates and iii) to investigate safeguard measures employed by them to mitigate the impacts of cyber-attacks as they interact with online activities.

This paper proceeds as follows. The related work provides valuable insights into the sources and category of cyber-threats, activity of cybercriminals and its attended impacts on unsuspecting victims. The remaining parts of the paper focus on research methodology, data collection and sampling techniques and statistical analysis. Interpretations and comprehensive discussions of the analyzed data corroborate the study with recommendations.

2. RELATED WORK

The use of various online platforms for financial transactions by the members of society and activities of cybercriminals has witnessed a tremendous increase, which has made many online users more susceptible to cyber threats (Salim et al., 2019). The susceptibility ranges from phishing email and identity theft, to malware and spam, to ransomware and spyware infections which can affect anybody and any infrastructure (Salim et al., 2019, Houssain *et al*., 2019, Maria *et al*., 2020). Houssain *et al* (2019) highlight top fifteen threats in 2018 in following order: Malware, Web-Based Attacks, Web Application Attacks, Phishing, Denial of Service (DoS), Spam, Botnets, Data Breaches, Insider Threat, Physical Manipulation/Damage/Theft/Loss, Information Leakage, Identity Theft, Ransomware and Cyber Espionage. The ranking of positions was based on the number of occurrences or incidences, impacts and connections to other cyber-attacks.

According to Houssain et al. (2019) there are two sources of threats, namely Threat agents and Attack vectors. Threat agents are the actors, individuals or organizations, who can create a threat. Examples of threat agents include hackers, cyber-criminals, insiders and nation-states. On the other hand, Attack vector is the route or means by which a threat agent gains access to a device or network for malicious activity (Houssain et al., 2019). Examples of attack vectors include web and browser attacks, internet exposed threat, mobile app stores, and malicious USB drives.

Victims of cyber-attacks can experience mental distress that can lead to depression. For instance, the emotional impact of identity theft on a victim could lead the person to become distressed and to feel violated, helpless, angry and betrayed (Maria *et al*., 2020). Others impact of cybercrime are the feelings of anger, pain, annoyance, being cheated and emotion of stress.

The activity of cybercriminals and its attended impacts can be assuaged. Houssain *et al*. (2019) suggest the following on some cyber-attacks: on Phishing, mitigation includes the education of potential targets about fake email, random clicking, and oversharing of private information while mitigation of Spam is through spam filters and user education. Mitigation against Web Application Attacks require policies for secure app development and for the authentication and validation of mechanisms while Identity Theft demands protection of documents, strong privacy settings on social media, password protection on devices, and care when using public WiFi.

3. METHODOLOGY

This study adopts survey research design and the schematic representation of the research methodology is as shown in figure 1. As discussed in section 2, extant literature reviews were carried out in order to identify various items for the study. For instance, category of cyber threats and safeguard measures are extracted from the work of Houssain *et al.* (2019) and Daniel *et al.* (2019) respectively. Online questionnaire and convenience sampling technique were found to be adequate for eliciting information from the respondents on the online payment modalities adopted during the lockdowns. Face and content validities were carried out in order to validate the research instrument. The face validity of the research instrument was established by ensuring that the items of the instrument are properly linked to the objectives of this study. This means that the questions on the questionnaire must help in the realization of the objectives. Moving beyond the physical appearance of the research instrument is the content validity. Content validity was done by thorough examination and inspection of all the items in the questionnaire by two experts in the field of cyber-security. The instrument also, contains 5-Likert scale measurement for the main research questions and the complete instrument is as shown in appendix A. In order to carry out a pilot test, the research tool was used to contact twenty Adeleke University staff. It was done prior to administering the final questionnaires online, to reveal if the format of the questionnaire and question items were suitable for achieving the objectives of the study.

The final data collection was done through online questionnaire that was made available to some volitional undergraduates in public and private universities in Nigeria via the Google Form between September 25 and October 10, 2020. Data collected were coded and entered into Statistical Package for Social Science (SPSS version 20) for data analysis. In order to test the internal consistency of the contents of the research tool, reliability test was carried out. Cross-tabulation or contingency table was used to display the relationships between two or more variables and significant levels of the variables were determined by Chi-square. One of the advantages of chi-square is that, it is appropriate for almost any kind of data. At the final stage, information was extrapolated from data analyzed from which recommendations and conclusions were made.

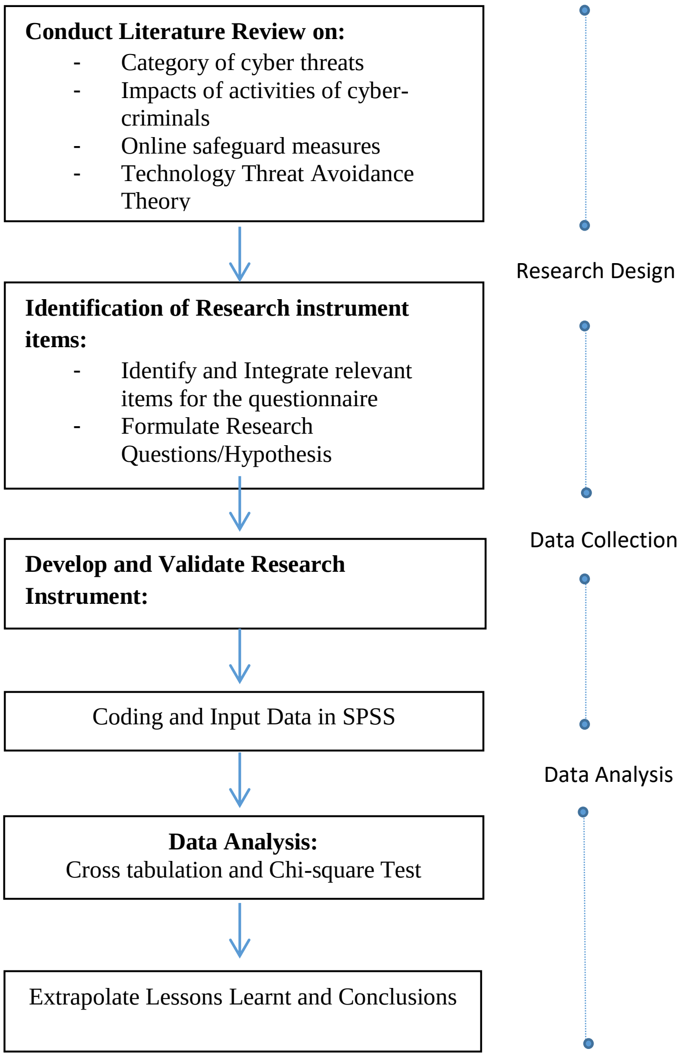
Conduct Literature Review on:
- Category of cyber threats
- Impacts of activities of cyber-criminals
- Online safeguard measures
- Technology Threat Avoidance Theory
Identification of Research instrument items:
- Identify and Integrate relevant items for the questionnaire
- Formulate Research Questions/Hypothesis
Develop and Validate Research Instrument:
Coding and Input Data in SPSS
Data Analysis:
Cross tabulation and Chi-square Test
Extrapolate Lessons Learnt and Conclusions
Research Design
Data Collection
Data Analysis

Figure 1: Research Methodology

4. RESULT AND DISCUSSION

4.1 Analysis of Demographic Characteristics

The sample of study is 118 participants, consisting of 55 male (46.6%) and 63 female (53.4). In addition, more than three quarters (78%) of the respondents were between the age group of 18-30 years and 98.3% of participants were from private universities.

Table 1: Demographic Information of the respondents

S/N	Items	Frequency	Percentage
Gender			
1	Male	55	46.6
2	Female	63	53.4
	Total	**118**	**100**
Age Group			
1	13-17 years	6	5.1
2	18-30 years	92	78.0
3	31-40 years	11	9.3
4	41 years and above	9	7.6
	Total	**118**	**100**
University			
1	Private	116	98.3
2	Public	2	1.7
	Total	**118**	**100.0**

In table 2, only 62.7% of the respondents have Antivirus on their computers and 44.9% on their mobile phones. 28% of the participants used licensed Antivirus while 41.5% used free Antivirus. This result shows that respondents tend to depend more on the use of free trial version of antivirus rather than licensed or paid antivirus, the act that may make them vulnerable to online attack.

Table 2: The use of Antivirus

S/N	Items	Frequency	Percentage
Availability of Antivirus on the Computer			
1	I do not	20	16.9
2	No	24	20.3
3	Yes	74	62.7
	Total	**118**	**100.0**
Availability of Antivirus on the Mobile Phone			
1	I do not	18	15.3
2	No	47	39.8
3	Yes	53	44.9
	Total	**118**	**100**
The use of paid or License Version of Antivirus			
1	I do not	30	25.4
2	No	55	46.6
3	Yes	33	28.0
	Total	**118**	**100**
The use of free trial Version of Antivirus			
1	I do not	22	18.6
2	No	47	39.8
3	Yes	49	41.5
	Total	**118**	**100**

Table 3 shows the mode of payments adopted by the respondents, with the highest (59.3%) coming from the use of Debit cards and Webpages. This high frequency suggests that most respondents embraced the use of Debit cards on webpages for online payments during pandemic.

Table 3: Mode of payment

S/N	Items	Frequency	Percentage
1	By entering the banking hall	6	5.1
2	By making payment via ATM	10	8.5
3	By transferring the payment to the university account via mobile phone	32	27.1
4	By using debit card via university portal	70	59.3
	Total	**118**	**100**

Also, the chi-square test (table 4) shows that there is significant relationship between age group 18 - 30 years and mode of payment (using debit card via university portal) at 0.05 level of significant. This suggests that the two variables are associated with each other.

Table 4: Chi-square test on Mode of payment

Age group (18-30 years) with Mode of payment (debit card and webpage)			
Item	**Description**	**Value**	**Asymp. Sig. (2-sided)**
1	Pearson Chi-Square	28.247	.001

Table 5 shows the values of Cronbach's alpha on Safeguard measure, Cyber-Treats, Impacts of cyber-attacks and Challenges with online payments. The table shows acceptable values of Cronbach's alpha. It reveals that the items included in the research tool demonstrated sufficient degree of internal consistency and that the research instrument developed is sufficient to realize the objective of the research.

Table 5: Reliability Statistics of the Data collected

S/N	Items	Cronbach's Alpha	Number of Items	Interpretation
1	Safeguard Measure	0.72	12	Good
2	Cyber-Treats	0.95	9	Excellent
3	The effects or impacts of Cyber-attacks	0.79	8	Good
4	Challenges with online payments	0.90	10	Excellent

4.2 Analysis of Categories of Cyber-threats

The participants were asked to indicate how often they experienced some listed categories of cyber-attacks or threats using 5-Likert scale measurement (Never = N, Rarely = R, Sometimes = S, Often = O, Always = A.). Their experiences are as follows: Spam (94.1%), Ransomware (87.3%), Malware (86.4%), Web Application Attacks (85.6%), Web-based attacks (84.7%), Denial of Service attacks (83.9%), Phishing (83.1%), Cyber-Espionage (82.2%) and identity theft (79.7%). Each of these categories is explained in Appendix A. None of these experiences is less than 50%; this suggests that the activities of cybercriminals were potent during the period under review.

Also, further analysis as shown in table 6, reveals that there are associations or relationships between i) gender and Cyber Espionage, ii) age and phishing and iii) age and Denial of Service respectively. These results are in agreement with report of Dawn *et al* (2020), that "younger adults (18–25 years) were found to be more susceptible to phishing attacks than any other age group prior to training."

Table 6: Chi-square test on Categories of Cyber-threats.

"Gender" with "Cyber Espionage"			
Item	**Description**	**Value**	**Asymp. Sig. (2-sided)**
1	Pearson Chi-Square	9.90	.042
"Age" with "Phishing"			
2	Pearson Chi-Square	23.56	.023
"Age" with "Denial of Service"			
3	Pearson Chi-Square	21.09	.049

4.3 Analysis of Impacts of activities of Cyber-criminals

The negative impacts of activities of cybercriminals have come to limelight (table 7) as online users recognized that cyber activities promote lack of trust among users (93%). This is followed by the activities of cybercriminals that has the possibility of causing depression (92%) with the belief that cyberattacks can cause damage to infrastructure (91%). Also, respondents state that cyberattacks have the possibility of discouraging one from using online payment (90%), causing embarrassment or shame (83%), damage relationships (76%), can cause loss of life (67%) and several online users had lost money to cybercriminals (45%). The findings in items 2 and 4 in table 7 are in conformity with the findings of Maria *et al*, (2020) which state that victims of cyberattack can suffer emotional trauma which can lead to depression and to the feeling of little interest in adopting new technology due to loss of confidence in online activities.

Table 7: Cross-tabulation table on Impacts of activities of Cyber- criminals

Item	Description	Agreed	Disagreed	Undecided
1	Cyber activity promotes lack of trust	110	2	6
		93%	2%	5%
2.	The activities of cybercriminals can cause depression	108	4	6
		92%	3%	5%
3	I belief Cyberattack can cause damage to infrastructure (e.g. computer or phone)	107	6	5
		91%	5%	4%
4	Cyberattack has the possibility of discouraging one from using online payment	106	1	11
		90%	1%	9%
5	Cyber activity can cause embarrassment or shame	98	4	16
		83%	3%	14%
6	Cyber activity can damage relationship	90	6	22
		76%	5%	19%
7	I belief cyberattack can cause loss of life	79	12	27
		67%	10%	23%
8	I had lost my money to cybercriminals before	53	45	20
		45%	38%	17%

4.4 Analysis of Safeguard measures employed by online users

In this empirical study, respondents were asked to respond to some listed basic safeguard measures expected of online users using 5-Likert scale measurement of strongly agreed, agreed, undecided , disagreed and strongly disagreed. The results are as shown in table 8.

Table 8 suggests that generally, respondents display positive or good attitudes before, during and after online transactions. But the negative attitudes of respondents are also revealed in items 10 and 12 with “I only give my password to my trusted friends” and “I can give my ATM card to my roommates to help me withdraw money’ respectively. This attitude of making confidential information known to friends stands condemned by all standards as this action has the possibility of breeding insider threats. Also, the responses of participants on item 6 -“I belief that my computer can be object of target online” is in conformity with study of Sri Devi *et al* (2019), which state that “hackers go after individuals, groups, businesses and government to steal critical IP and national secrets”

Table 8: Cross-tabulation table on Safeguard measures

Item	Description	Agreed	Disagreed	Undecided
1	I belief protecting my computer is necessary	116	0	2
		98%	0%	2%
2.	I use safeguard measure (e.g. password) to prevent unauthorized person from accessing my computer	115	0	3
		97%	0%	3%
3	I always ensure I use secured webpage for my online payments	108	4	6
		92%	3%	5%
4	I use strong password (alphanumeric and special character)	106	3	9
		90%	3%	8%
5	I use safeguard measure (e.g. antivirus) because I belief my computer can be attacked by virus	104	2	12
		88%	2%	10%
6	I belief that my computer can be object of target online	104	6	8
		88%	5%	7%
7	I always close my browser or the webpage whenever I carried out online payment	99	4	15
		84%	3%	13%
8	I always logout from my email whenever I use it in public places	98	4	16
		83%	3%	14%
9	There is benefit in updating password regularly	97	3	18
		82%	3%	15%
10	I only give my password to my trusted friends	81	11	26
		69%	9%	22%
11	I always activate my browser firewall	73	12	33
		62%	10%	28%
12	I can give my ATM card to my roommates to help me withdraw money	62	28	28
		53%	24%	24%

Consequently, in table 9, chi-square test reveals that there are significant associations between variables Age with “I give my password to trusted friends” and Age with “I belief that my computer can be object of target online” respectively. This implies that respondents seem unmindful or unaware of the cybersecurity risks posed by their deliberate actions. Therefore, respondents need more educational programmes on the revelations of activities of cybercriminals.

Table 9: Chi-square test on Safeguard Measures

“Age” with “I give my password to trusted friends”			
Item	**Description**	**Value**	**Asymp. Sig. (2-sided)**
1	Pearson Chi-Square	28.90	.004
Age with I belief that my computer can be object of target online			
2	Pearson Chi-Square	32.92	.001

4.5 The increase or otherwise in the activities of cyber-criminals during Covid-19 Pandemic

On the issue of increase or otherwise of the activities of cyber-criminals and the attended impacts during Covid-19, out of 118 respondents, 22 (19%) stated that they did not know if it was on increase, 4 (3%) responded “No” - it was not on increase and 92 (78%) stated “Yes” that activities of cyber-criminals were on increase during the said period.

This finding is in conformity with study of Sri Devi *et al* (2019), who state that “the number of cyber-attacks and threats has increased substantially in recent years, and hackers go after individuals, groups, businesses and government to steal critical IP and national secrets.”

5. CONCLUSION

Our investigation showed that respondents experienced Spam, Malware, Web-application attacks, Phishing and Identity thefts among other attacks during the lockdowns. 78% of the respondents stated that activities of cyber-criminals were on increase during lockdowns. We conclude that from a safety perspective, this study emphasizes the use of safeguard measures such as the use of strong passwords, secured webpage, licensed antivirus, keeping the PIN number and password secret by every online user are very crucial to mitigate the activities of cybercriminals.

6. RECOMMENDATIONS

Our recommendations are as follows:

i) The activity of cybercriminals is on increase therefore, there should be increased in cybersecurity awareness programmes among undergraduates;

ii) Every online users should adhere to basic cyber security safeguard measures such as using licensed antivirus, the use of strong password, keeping password and PIN number secret;

iii) There should be more enlightenments on the important and advantages of using of licensed antivirus. If possible university administrators can make licensed multiusers antivirus available for their students;

iv) The attitude of making passwords and PIN numbers known to friends stands condemned by all standards as this action has the possibility of breeding insider threats;

v) The attitude of updating passwords regularly should be sustained by all online users;

7. REFERENCES

Daniel Qi Chen and Huigang Liang (2019): Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory. IEEE Transactions on Engineering Management, vol. 66, No. 4, November 2019

Dawn M. Sarno, Joanna E. Lewis, Corey J. Bohil and Mark B. Neider (2020): Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. Journal of Human Factors and Ergonomics Society. ol. 62, No. 5, August 2020, pp. 704–717. DOI: 10.1177/0018720819855570

Farringer R Deborah 2019: Maybe If We Turn It Off and Then Turn It Back On Again? Exploring Health Care Reform as a Means to Curb Cyber Attacks. The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s) DOI: 10.1177/1073110519898046

Houssain Kettani and Polly Wainwright (2019): On the Top Threats to Cyber Systems. 2019 IEEE 2nd International Conference on Information and Computer Technologies. DOI: 10.1109/INFOCT.2019.8711324

Maria Bada and Jason R. C. Nurse (2020): The Social and Psychological Impact of Cyber-Attacks. To be published in: Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press

Salim A. Mouloua, James Ferraro, Mustapha Mouloua, Gerald Matthews and Robert R. Copeland (2019): Trend Analysis of Cyber Security Research Published In HFES Proceedings from 1980 To 2018. Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting DOI 10.1177/1071181319631467

Appendix A

Section A: Background Information

1. Gender?

Male	Female

2. Age group?

13-17	18-30	31-40	41 and above

3. University?

Public	Private

4. Level?

100	200	300	400	500

5. What mode of payment did you use **most** during COVID 19? (Kindly pick one)

1	By entering the banking hall	
2	By transferring the payment to the university account via my mobile phone	
3	By making payment via ATM	
4	By using credit card via university portal	

6. Do you have antivirus on your computer to protect it?

Yes	No

7. Do you have antivirus on your Mobile phone to protect it?

Yes	No

8. Do you use paid or licenced version of antivirus?

Yes	No

9. Do you use free trial version of antivirus?

Yes	No

Section B: Please choose the option that best describes your feeling or opinion as regards the statements presented in this table.

1. Which of these safeguard measures do you use? Mark the appropriate options from Strongly Agreed (SA), Agreed (A), Undecided (U), Disagreed (D) and Strongly Disagreed (SD).

S/N	Safeguard measure	SA	A	U	D	SD
i)	I belief protecting my computer is necessary					
ii)	I use safeguard measure (e.g. antivirus) because I belief my computer can be attacked by virus					
iii)	I use safeguard measure (e.g. password) to prevent unauthorised person from accessing my computer.					
iv)	I only give my password to my trusted friends					
v)	There is benefit in updating password regularly					
vi)	I belief that my computer can be object of target online					
vii)	I can give my ATM card to my roommates to help me withdraw money					
viii)	I use strong password (alphanumeric and special character)					
ix)	I always activate my browser firewall					
x)	I always logout from my email whenever I use it in public places					
xi)	I always close my browser or the webpage whenever I carried out online payment					
xii)	I always ensure I use secured webpage for my online payments.					

2. Which of these cyber-attacks or threats did you experience? Mark the appropriate options from Never = N, Rarely = R, Sometimes = S, Often = O, Always = A

S/N	Cyber-threats	N	R	S	O	A
1.	**Malware:** is software with a malicious intent to destroy a computer, server, or network	1	2	3	4	5
2.	**Web-Based Attacks** make use of web-enabled systems such as browsers, webpages, and content managers.	1	2	3	4	5
3.	**Web Application Attacks**: take advantage of Application Programming Interfaces (APIs) which are exposed and open.	1	2	3	4	5
4.	**Phishing:** a type of fraud in which fraudulent emails are sent to steal personal data, including login credentials and banking information.	1	2	3	4	5
5.	**Denial of Service Attacks:** occur when machine or network resources are made unavailable to their intended users by disrupting service	1	2	3	4	5
6.	**Spam:** is flooding users with unsolicited messages by email and messaging technologies	1	2	3	4	5
7	**Identity Theft**: is obtaining information about a person or computer system for the purpose of impersonating the target	1	2	3	4	5
8.	**Ransomware:** is Malware that encrypts files or locks down a system until the target pays the actor to remove the restrictions.	1	2	3	4	5
9.	**Cyber Espionage**: involves the use of a computer network to obtain confidential information	1	2	3	4	5

3. What are the effects of cyber-attacks or threats? Mark the appropriate options from Strongly Agreed (SA), Agreed (A), Undecided (U), Disagreed (D) and Strongly Disagreed (SD).

S/N	Impacts or Effects	SA	A	U	D	SD
1	I belief cyberattack can cause loss of life					
2	I belief Cyberattack can cause damage to infrastructure (e.g. computer or phone)					
3	I had lost my money to cybercriminals before					
4	The activities of cybercriminals can cause depression					
5	Cyber activity can damage relationship					
6	Cyber activity can cause embarrassment or shame					
7	Cyberattack has the possibility of discouraging one from using online payment					
8	Cyber activity promotes lack of trust					

4. Can you say that the activities of cyber-criminals are on increase during COVID-19 pandemic?

Yes	No	I don’t know

Author’s Brief Profile

Onamade, A. Abraham (PhD) is currently a lecturer in the Department of Computer Science, Adeleke University, Ede, Osun State, Nigeria. His research areas include Health Informatics and Telemedicine. He can be reached by phone on +1347030667893 and through E-mail onamadeakintoye@gmail.com

Sokoya O. Samuel holds BSc in Mathematics from Chartered Oak State College USA, MSc in Information Security and Assurance from Western Governors University USA. He is a PhD student in Information Technology at the Department of Computer Information Sciences, University of the Cumberlands, 6178 College Station Drive Williamsburg, KY 40769 and his research interest is in Cyber Security. He can be reached by phone on +1 909-583-4120 and through E-mail daresokoya@gmail.com

Oduwole, O. Ayodele hails from Ile-Ife, Osun State. He holds a Bachelor of Technology (B. Tech.) degree in Mathematics / Computer Science and a Master of Technology (M. Tech.) degree in Computer Science. He is a lecturer in the Department of Computer Science, Adeleke University, Ede, Osun State, Nigeria, where is currently pursuing his PhD in Computer Science. He can be reached by phone on +234 803 440 8158 and through E-mail dayooduus@yahoo.com

Adegbite, Oluwaseyi holds a Bachelor of Technology (B. Tech.) and a Master of Science (M.Sc.) degree in Computer Science. He is currently on his PhD at Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria. He is presently lecturing in the department of Computer Science, Adeleke University, Ede, Osun State, Nigeria. His research areas include E-health and Telemedicine. He can be reached by phone on +234 803 791 8201 and through E-mail sheykole@gmail.com