Nigerian Journal of Technology (NIJOTECH)
Vol. 42, No. 2, June, 2023, pp.249 - 256
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v42i2.13

AN APPROACH TO CYBERCRIME ISSUES IN DANDUME LOCAL GOVERNMENT AREA OF KATSINA STATE, NIGERIA

J. Garba[1,*]

[1]College of Computing, Informatics, and Media, Universiti Teknologi Mara Malaysia.

*corresponding author (Email: jamilugarba2223@gmail.com)

Article history: Received 21 March, 2023. Revised 10 May, 2023. Accepted 26 May, 2023. Published 31 July, 2023. ***CC BY-NC-ND Licence***

Abstract

This study investigated cybercrime issues in Dandume Local Government Area of Katsina State. The study aimed to understand the various types of cybercrimes that the community faces and the resulting impacts, particularly educational and psychological effects on the victims. Additionally, the study discussed the main causes of these crimes, particularly among young people. To achieve these aims, the study collected data from 115 residents of Dandume using a structured questionnaire. The collected data was analyzed using statistical tables. The results showed that cybercrime is prevalent in the Dandume community, with many of the participants reporting that they had experienced one form of cybercrime or the other. The most common types of cybercrime reported by the participants were yahoo attack, social media hijacking, credit card threat, government offer scam, and airtime scam. Furthermore, the study revealed that many of the participants were not aware of the various ways they could protect themselves from cybercrime. Furthermore, the study highlighted the effects of these crimes on the victims and discussed the main causes of cybercrimes among users of internet in the area. The paper made some recommendations for minimizing the challenges of cybercrime in Nigeria. The study underscored the importance of community education and awareness-raising on the dangers of cybercrime and suggests the need for increased efforts to implement security measures to protect residents from cybercriminals.

Keywords: Cybercrime, Rural communities, Dandume, Katsina state, Nigeria.

1.0 INTRODUCTION

The emergence of information and telecommunication technology, ICT especially the internet has eased our daily activities. In recent times, internet or web-enabled phones and other devices have made internet access easier and faster [1]. Individuals, organizations, businesses are benefiting with variety of opportunities such as sorting of data, summarizing, coding, editing, customized, minimising spaces and generating report in Realtime. These have helped to save time, money, and efforts from operational perspective [2]. These technological advancements gave birth to modern communication tools that use and process all those kinds of data. Organizations substantive businesses and society at large rely on ICT [3]. Computers and information sharing have almost completely taken over human life in recent years.

Despites all these opportunities, unfortunately, ICT has also led to varieties of challenges bedevilling the society such as criminal activities, spamming, credit card frauds, ATM frauds, password sniffing, phishing, and identity theft [4]. In Nigeria, all these forms of internet related crimes and frauds are known as ‘yahoo-yahoo’ or ‘419’. The term "yahoo" comes from the early days of the scam when perpetrators used Yahoo email accounts to carry out their fraudulent activities. The term "yahoo" has become a slang term in Nigeria for internet fraudsters or scammers. Thus, "yahoo attacks" refer to cyber-attacks or hacking carried out by Nigerian scammers or fraudsters using the same tactics as the “Yahoo Yahoo” scams.

Thus, it can be said that while emergence of ICT and internet penetration access has created positive opportunities for individuals, organizations and businesses activities, it has on the other hand provide negative opportunities to those that engage in illegal activities [5]. The rise of ICT and online communication has resulted in a significant rise in the prevalence of criminal activities as well as the creation of what seems to be a new category of criminal activity. Both the increase in the incidence of criminal activities and the possible creation of new category of criminal activities pose challenges for organizations, and businesses, as well as for law enforcement agencies. However, different people with different perspectives are discussing the issue and challenges of cybercrime. The problem is not limited to Nigeria and other third world countries; even technologically developed nations like the United States, cybercrime has advanced beyond traditional crimes and now poses a threat to national security [6]. According to the annual report of Internet Crime Complaint Centre [7], Nigeria ranked as the 16th cybercrime complain in the world.

Cybercrime is seriously challenging in Nigeria and are carried out online which makes it difficult to detect by the police. The absence of strong law makes policing even more difficult. Creation of laws against cybercrime activities could be the influencing factor against such activities. According to [8] The continual use of the internet by immoral cyberspace users to commit crimes over the past 20 years has caused a growing feeling of fear among the general public as well as conflicting thoughts of fear for organization and businesses. Recently, this phenomenon has grown increasingly complex and has called for quick response in providing laws that would protect the cyberspace and its users. The Nigeria National Assembly passed the Cybercrimes (Prohibition, Prevention, Etc) Act in 2015, which was then signed into law by the president. This law serves as a comprehensive legal, regulatory, and institutional framework for preventing, detecting, and punishing cybercrimes in Nigeria. Additionally, it offers protection for critical national information infrastructure and promotes cybersecurity and the safeguarding of computer systems and networks, electronic communications, data, computer programs, intellectual property, and privacy rights. However, there has been poor implementation of the existing law against cybercrime in the country; thus, individuals and businesses take responsibility for the safety of their cyber environment [9].

The rise of cybercrime has become a significant challenge for many communities around the world, and the Dandume community of Katsina State, Nigeria is no exception. With the increasing use of technology in today's society, cybercrime has become a prevalent issue affecting individuals, businesses, and governments. In lieu of this, the paper will explore an approach to addressing cybercrime issues in the Dandume community of Katsina State, Nigeria. The study will focus on identifying the different types of cybercrime affecting the community, analysing the root causes, and proposing effective solutions that can help mitigate the impact of cybercrime on individuals and businesses in the community.

1.1 Cybercrime in Dandume Local Government

Nigeria is among the developing countries in Africa, with wide internet penetration in almost all sections of the country. Social media, online shopping, or money transfer, everything is only a click. Furthermore, as the number of internet users grow, many users become victims of various cyber-attacks while spending a lot of time on the cyber environment [10]. Many reasons could be the influencing factors for the rise of cybercrime in many parts of Nigeria. Lack of cybersecurity awareness and education are among of those reasons that lead many users become victim to cybercrimes. It has been observed that while cybercrime rises, detection rates remain very low. A number of times, several criminal cases have been published by Economic and Financial Crime Commission (EFCC) in the country. Criminals takes the advantage of lack education and predominated in many part of the country on social media to trick people with many techniques to reveal their sensitive information.

1.2 Causes of Cybercrime in Dandume Local Government

The world of communication has undergone a significant transformation as a result of technological advancements in the global telecommunications infrastructure, including computers, mobile phones, and the internet. People of all ages and socioeconomic backgrounds in Nigeria use the internet to communicate with one another and as well, access information more quickly and easily. However, the prevalence of cybercrime is a negative side of this development [11]. Internet penetration in Nigeria keeps growing. According to the Internet World Statistics Report (IWS, 2021), Nigeria has a population of 211 million, of which 101 million are internet users, with 73% of this population accounting for internet penetration. Researchers in Nigeria have identified a number of factors as the primary and fundamental causes of cybercrime. Some of the identified reasons of cybercrime are as follows [12]:

a. **Unemployment:** High rate of unemployment is among the main and major causes of cybercrime among the youth in Nigeria. High rate of unemployment in Nigeria comes with many challenges that includes socioeconomic, political, and national security consequences. And this accounts for the rise of street youths that grow up in a culture that encourages criminal behaviour. Additionally, those unemployed youths have plenty of free time and easy access to the internet, allowing them to engage in cybercrime. Even if they do not have Internet access at home, cyber-cafés are widely accessible in the country and provide Internet access.

b. **Poverty:** Another factor leading to the rise of cybercrime in Nigeria is poverty. According to Umar (2020), poverty means not having adequate food, shelter, clothing, and enjoyment. And the absence of all these necessities of life can unintentionally turn people into criminal activities such as cybercrime for their survival.

c. **Quest for wealth:** Quest for wealth is another reason behind many cybercrime problems in Nigeria. Young people today are lazy, and they are not ready to start a small business with available capital, so they fall into criminal activities because cybercrime requires the little guidance with very little capital. The Get Quick Rich Syndrome has been one of the reasons for the hike in the number of cybercrimes in the country.

d. **Lack of implementation of cybercrime law:** Another major cause of cybercrime in Nigeria is the poor implementation of the existing cybercrime laws. Though Nigeria has the legal framework that caters for the punishment and preventions of cybercrime, the poor execution and implementation of same laws continue to encourage cybercriminals for committing more cybercrimes because they know that the criminals would go unpunished even when they are caught. Therefore, Nigerian government with collaboration of some private organization need to develop a strong framework for the implementation of cybercrime laws so that cybercriminals would get punished and such punishment would deter others from committing the crime.

1.3 Various Types of Cybercrime in Dandume Local Government

There are several types of cybercrimes that are committed daily in Nigeria and also in the world through various forms of techniques. Some of the cybercrime that are prevalence In Dandume are discussed below:

a. **Yahoo attack (also called 419):** This type of cybercrime is well-known in Nigeria. Nigerian cybercriminals are known for using spam emails, money-laundering emails, and cleverly crafted but pretend company partnership offers to trick people into falling for fraudulent scams. The term "yahoo boys" refers to criminals who engage in the advance fee fraud schemes (419) known as “yahoo boys”. This type of crime combines impersonation, obtaining by false pretence or advance fee fraud (AFF). The biggest trick of this scam is a calculated persuasion. Victims often stick to logical persuasion after the scammer guesses their mindset for every action to take. Lured by these well-crafted lies, victims end up losing large sums of money or revealing their credit card numbers or banking passwords.

b. **Credit card / ATM fraud:** This includes illegal or unauthorized use of people's credit/debit cards to steal their money. Due to negligence or recklessness, victims often pass their credit/debit card numbers to fraudsters who obtain the same numbers through careful observation or outright theft, sometimes under threat of 'a weapon. In Nigeria, such a number is obtained at an ATM anywhere or at a robbery withdrawal terminal, and a pin is obtained on a gun. According to [13], Nigerian depositors and banks lose N6.2 billion in one year to cybercrime, mostly related to online banking and credit card/ATM fraud.

c. **Social media hijacking:** This is another type of crime that arises in modern social platforms. There are variety of issues of hijacking social media accounts by hackers, and most of the time the hackers demanding of ransom before releasing the account. In some cases, some social media accounts have been used by the hackers especially those account with number of followers. This type of crime mostly occurred in Facebook, Instagram, and twitter. This crime involves sending messages asking for money or other help from authorized accounts to friends and family. Another common scenario also occurs when scammers create social media accounts pretending to be other people, especially celebrities.

d. **Bank verification number (BVN) scams:** In 2014 the central bank of Nigeria (CBN) introduced a centralized biometric identification system which known as Bank Verification Number (BVN). The BVN consists of 11-digit number that acts as a universal ID across all the banks in Nigeria. It was introduced to link various accounts to the owner and to protect bank's customers from identity theft and other related cyber offences [14]. This type of crime gave rise when the Central Bank of Nigeria (CBN) made the announcement of deadline for Bank Verification Numbers (BVN). Cybercriminals impersonating legitimate bank employees began contacting bank customers, requesting their bank account information, and promising to help them unlock their accounts, and this resulted in huge financial damages.

e. **Government grant scams:** Scammers can trick you on social media by sending a message that appears to be from one of your social media "friends," telling you they received a grant from the government and that you should apply, too. To receive the grant, all you have to do is share your address, date of birth, driver's license information and then pay a fee to receive the funds. Once you provide the information the scammer requests and pay the fee, you will not receive the phony grant. Instead, you have opened the door to identity theft and financial fraud.

f. **Data and airtime theft from service providers:** Such crimes occur among young people in Dandume local government and across the country. They illegally access "cheat codes" and use them illegally to get thousands of mobile data and unlimited airtime without paying the required fees. Internet cafes have also developed ways to connect to ISP networks [15].

1.4 Impact of Cybercrime Dandume Local Government

The emergence of information and communication technology brought many opportunities to users and organization at whole, makes life easy, along it comes with some challenging through cybercrimes that have negative impact among users in Dandume. There are many negative impacts of cybercrime but this paper focusing on those that have effect on people in Dandume local government. Below are some of those negative impacts of cybercrime [16].

a. **Financial loss:** financial loss is among the negative impact of cybercrime, there many statics of various loses cause as a result of cyberattacks. Organization and users are seriously suffering from cyberattacks.

b. **Psychological effect:** cybercrime victims some suffer from emotional trauma, which in most cases lead to depression. Cybercrime activities increases fear in the mind of the victim, therefore it very important to enhance the cybersecurity measures to avoid psychological challenges among the victims.

c. **Educational effect**: The emergence of social media made it simple for young people in Nigeria to become aware of cybercrime. The desire to engage in cybercrime has significantly increased as a result of people becoming more aware of the risks associated with wealth after seeing the luxury style of life that is prevalent on social media, in clubs, and at other social gatherings, and this led the people are withdrawing from school and join the cybercriminal activities.

1.5 Possible Solutions to Minimize Cybercrime

There are different approaches provided by researchers and security experts. Below are some of the possible solutions to cybercrime by [17]:

a. **Provision of jobs by government:** As the government sees public servants' loots with taxpayers' money, it must create jobs opportunities for the growing number of unemployed young people who believe that cybercrime is the only way to survive and get rich quick. This will help minimize the cyberthreat.

b. **The need for individuals to observe simple rules:** Internet users must ensure adequate protection against all forms of cybercrimes and malware on their computer systems. They should avoid pirated versions of the software, never reveal bank account sensitive information, personal identification number (PIN), email (password) with strangers.

c. **Security education training and awareness (SETA):** Cybersecurity education, awareness and training program are the most important weapon for literacy because such education, training and awareness should be organized from time to time with a focus on cybersecurity so that individuals should learn how protect their personal information and that people are safe from cybercrime.

d. **Cyber ethics and cyber law:** Cyber ethics and cyber laws are also designed to minimize the prevalence of cybercrimes in Nigeria and around the world. It is the responsibility of every individual to comply with cyber ethics and cyber laws in order to reduce the growing cybercrime.

2.0 RESEARCH METHODOLOGY

The purpose of this study is to assess the prevalence of cybercrime in Dandume, Katsina State. The study adopted descriptive survey method and quantitative research design. Quantitative methods deal with the numerical form of data obtained from respondents. The research instrument used for the study is the structured questionnaire which was segmented into two sections. Section A deals with demographic profile of the respondents while the second section ask questions related to the study objectives. The questionnaire was administered using online platform to residents of Dandume Local Government, Katsina State. This was in order to get a broad range of responses from different categories of internet users' resident in the study area. A total of 115 respondents participated in this survey and the results analysed are shown in the following section.

3.0 DATA ANALYSIS AND DISCUSSION

This section deals with the analysis of the data obtained from the field work through the administered questionnaire. Data collected from the respondents are presented, analysed and interpreted statistically using tables and percentage.

3.1 Respondents' Demographic Information

Table 1: Respondents' demographic information

Gender	**Frequency**	**Percent**
Male	85	73.9%
Female	30	26.1%
Age	**Frequency**	**Percent**
18 to 25	29	25.2%
26 to 35	63	54.8%
36 to 45	22	19.1%
46 to 55	1	0.9%
Above 55	-	-
Occupation	**Frequency**	**Percent**
Farming	35	30.4%
Business	36	31.3%
Studying	44	38.3%
Educational qualification	**Frequency**	**Percent**
PhD	-	-
Master's degree	8	7%
Bachelor's degree (B.Sc./HND)	60	7%
Diploma/NCE	39	33.9%
Secondary school graduate	8	52.2%
Total	**115**	**100%**

Table 1 above shows that majority of the participant in this survey are male with the frequency of 85 and 73.9%, while that of female is total frequency of 30 and 26.1%. However, most of the participant are young this is because the issue of cybercrimes mostly associated with young and also the young people have highest percentage in cyberspace. The highest number of participants in this survey are student. Also, majority of the participants are secondary school graduate.

3.2 Cybercrime Issues in Dandume Local Government

This section will discuss the cybercrime is case study area. Starting with the various types of cybercrime in that area, what are the effect of those crime among the citizens, what are the major cause of those crimes, and also the solutions that need to apply to minimize the cybercrime challenges.

The 5 Likert scale was used to rank the participant opinion. Strongly agree (SA), Agree (A), Neutral (N), Disagree (DA) and Strongly Disagree (SDA).

Table 2: Various types of cybercrime in dandume local government

S/N	**Types of Cybercrime**	**Response**	**Level of Agreement**				
			SDA	**D**	**N**	**A**	**SA**
1	Yahoo attack (also called 419)	**N**	5	7	2	22	79
		%	4.3%	6.1%	1.7%	19.1%	68.8%
2	Credit card /ATM fraud	**N**	5	5	14	48	43
		%	4.3%	4.3%	12.3%	41.7%	37.4%
3	Social media account hijacking	**N**	6	6	7	37	59
		%	5.2%	5.2%	6.1%	32.2%	51.3%
4	Bank verification number (BVN) scams	**N**	8	4	11	43	49
		%	7.0%	3.4%	9.6%	37.4%	42.6%
5	Government offers scams	**N**	5	9	9	39	53
		%	4.3%	7.8%	7.8%	34%	46.1%
6	Data and airtime theft from service provider	**N**	4	7	10	29	65
		%	3.4%	6.1%	8.8%	25.2%	56.5%

From Table 2 that majority of respondents (87.9%) pointed out that Yahoo attack (also called 419) is the most various types of cybercrime in Dandume local government, 10.4% of the participants disagree with this opinion, while the remaining percentage (1.7%) of the participants are neutral. Theft of data and airtime from service providers was also reported at 81.7%, one of the most various forms of cybercrime in Dandume local government, with only a few respondents, 9.5% the denying and others (8.8%) neutral participants. Similarly, enough respondents (83.5%%) supported that social media account hijacking is among the various types of cybercrimes.

Government offers scams was also declared by 80% of the participants that is one among the various types of cybercrime in Dandume local government. Bank verification number (BVN) scams is another types of cybercrime in Dandume local government, the results show that (80%) of the participants responded positively to this, and also 10.4% disagreed with this, while the reaming participants of 9.6% are neutral. Similarly, Credit card /ATM fraud is (79.1%) supported this as the various types of cybercrimes in Dandume local government, 12.3% remained neutral, while the remaining percentage (8.6%) of the participants negated this as the various types of cybercrime in Dandume local government.

Table 3: Impact of cybercrime in dandume local government

S/N	Effects of Cybercrime	Response	Level of Agreement				
			SDA	D	N	A	SA
1	Financial losses	N	5	11	5	19	75
		%	4.3%	9.6%	4.3%	16.6%	65.2%
2	Psychological impact	N	7	8	19	33	48
		%	6.1%	7%	16.5%	28.7%	41.7%
3	Educational impact	N	6	11	18	30	50
		%	5.2%	9.6%	15.6%	26.1%	43.5%

Table 3 shows that the majority of participant in this survey (78.8%) agreed that financial losses is among the impact of cybercrime in Dandume local government, 13.9% participants disagree with this opinion, and the remaining percentage of 4.3% of the participant were neutral. Significant of (69.6%) of participant said that cybercrime also cause educational impact among the victims. Also, few participants (14.8%) negated this opinion, and the reaming (15.6%) are neutral. Psychological impact is another effect of cybercrime in Dandume local government, the result from the table indicated that the majority of (70.4%) of participant responded positively to this, and (14.8%) disagreed with this, while the remaining percentage (15.6%) of the participants are neutral.

Table 4: Causes of cybercrime in dandume local government

S/N	Causes of Cybercrime	Response	Level of Agreement				
			SDA	D	N	A	SA
1	Unemployment	N	7	4	5	12	87
		%	6.1%	3.4%	4.3%	10.5%	75.7%
2	Quest of wealth	N	6	5	13	38	53
		%	5.2%	4.3%	11.3%	33.1%	46.1%
3	Poverty	N	8	4	6	36	61
		%	7%	3.4%	5.2%	31.3%	53.1%
4	Lack of strong cybercrime law	N	6	7	7	30	65
		%	5.2%	6.1%	6.1%	26.1%	56.5%

The researcher again wanted to examine the causes of cybercrimes in Dandume local government. The result from Table 4 shows that 86.2% of participants said that unemployment among youth people is major cause of cybercrime in Dandume local government, 9.5% of the participants negated this opinion, while the remaining participants of 4.3% are neutral. A significant participants (82.6%) responded that lack of strong cybercrime law will be the cause of prevalence of cybercrime, because law can discourage people from participating in any crime. A sufficient number of participants (84.4%) said that poverty can also led young people to participate in crime, especially for cybercrime that needed less capital to start. 79.2% of participants responded to Quest of wealth as among the causes of cybercrime in Dandume local government, because our young people need to become rich in short period of time without hardworking, and this could lead them to various types of crimes including cybercrime.

Table 5: Solutions to cybercrime dandume local government

S/N	Solutions to Cybercrime	Response	Level of Agreement				
			SDA	D	N	A	SA
1	Job creation of govern-ent	N	9	2	4	19	81
		%	7.8%	1.7%	3.4%	16.6%	70.5%
2	The need for individual to observe simple rules	N	5	6	10	52	42
		%	4.3%	5.2%	8.8%	45.2%	36.5%
3	Security education training and awareness (SETA)	N	7	4	1	17	86
		%	6.1%	3.4%	0.9%	14.8%	74.8%
4	Cyber ethics and strong cyber law	N	6	6	6	39	58
		%	5.2%	5.2%	5.2%	33.9%	50.5%

The result of table 5 indicate that majority of respondents (89.6%) supported that Security education training and awareness (SETA) is among the solutions to minimize cybercrime in Dandume local government, also few participants (9.5%) nagged this solution and the remaining (3.4%) of the participants are neutral. Job creation of government pointed out by (87.1%) participants as among the solution to curb the cybercrime challenges. However, (84.4%) participants supported that creation of cyber ethics and strong cyber law could be the influencing factors to minimize the issues of cybercrime. Similarly, a sufficient number of participants (81.7%) said that the need for individual to observe simple rules also help to minimize the issues, and also 9.5% of the participants negated this opinion, while 8.8% of the participants remain neutral

4.0 CONCLUSION AND RECOMMENDAT-ION

4.1 Conclusion

In conclusion, the data collected in this survey reveals that cybercrime is a significant problem in Dandume community. The results indicate that Yahoo attack, theft of data and airtime from service providers, social media account hijacking, government offers scams, Bank verification number (BVN) scams, and credit card/ATM fraud are among the types of cybercrime found in Dandume local government. These crimes have a significant impact on the citizens, including financial losses, psychological effects, and damage to reputation and social status. From the demographic information of the survey found that most of the respondents are male and also young people between the age of 26 to 35.

The majority of the participants in the survey are male, and most of them are secondary school and Diploma/NCE graduate. The high level of education among the participants indicates that awareness and education on cybercrime are essential in the fight against cybercrime in Dandume local government. The most common types of cybercrime reported in this study were Yahoo attack, theft of data and airtime from service providers, social media account hijacking, government offer scams, Bank Verification Number (BVN) scams, and Credit card/ATM fraud.

The participants agreed that cybercrime had negative impacts on their financial status, psychological well-being, and social life. The findings of this survey indicate that there is a need for more awareness and education on cybercrime prevention and security measures in Dandume local government. The government, law enforcement agencies, and other stakeholders should work together to develop effective strategies and policies to combat cybercrime and protect the citizens' interests.

4.2 Recommendations

Based on the findings of the study on cybercrime issues in Dandume community of Katsina State, Nigeria, the following recommendations are suggested:

1. There is a need to create awareness among the residents of Dandume community about the dangers of cybercrime and how to identify and prevent it. Awareness campaigns could be organized in collaboration with local authorities, schools, and other stakeholders to educate people on the dangers of cybercrime and how to stay safe online.

2. There is a need for improved infrastructure, such as the provision of reliable internet services, to enable residents to access online services securely. This can be achieved through partnerships with internet service providers or government agencies responsible for internet access.

3. The Nigerian government should enforce cybersecurity laws and regulations to ensure that cybercriminals are brought to justice. This would serve as a deterrent to others and help reduce the incidence of cybercrime in Dandume community and other rural areas.

4. Because the country's high unemployment rate has contributed significantly to the rise in cybercrime, it is very important for the government and organizations to create jobs for the youths and provide security education and awareness through different procedures and methods in order to minimize the cybercrime challenges in Dandume local government.

5. Young people in Dandume community should be empowered with digital skills to enable them to use the internet safely and productively. This can be done through training programs and collaborations with youth organizations in the community.

6. Professionals such as law enforcement officers and teachers should be provided with cybersecurity training to enable them to identify and prevent cybercrime in their communities.

7. Collaboration among relevant stakeholders such as law enforcement agencies, schools, and internet service providers are necessary to address cybercrime issues in Dandume community. This can be achieved through the establishment of a cybersecurity task force or committee to coordinate efforts in preventing and combating cybercrime in the community.

REFERENCES

[1] Olubukola, S. “Cybercrime and Poverty in Nigeria,” *Can. Soc. Sci.*, vol. 13, no. 4, pp. 19–29, 2017, doi: 10.3968/9394.

[2] Ugwuja, V. C. “Cyber Risks in Electronic Banking: Exposures and Cybersecurity Preparedness of Women Agro-entrepreneurs in South- South Region of Nigeria,” *J. Bus. Divers.*, vol. 20, no. 3, 2020, doi: 10.33423/jbd.v20i3.3087.

[3] Chowdhury, N. H., Adam, M. T. P., and Teubner, T. “Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures,” *Comput.*

Secur., vol. 97, p. 101963, 2020, doi: 10.1016/j.cose.2020.101963.

[4] Al-shanfari, I., Yassin, W., and Abdullah, R. “Identify of Factors Affecting Information Security Awareness and Weight Analysis Process,” *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 534–542, 2020, doi: 10.35940/ijeat.c4775.029320.

[5] Stewart, H., and Jürjens, J. “Information security management and the human aspect in organizations,” *Inf. Comput. Secur.*, vol. 25, no. 5, pp. 494–534, 2017, doi: 10.1108/ICS-07-2016-0054.

[6] Odunayo, E., and Frank, I. “Approach to cybersecurity issues in Nigeria: challenges and solution,” *Int. J. Cogn. Res. Sci. Eng. Educ.*, vol. 1, no. 1, 2013.

[7] IC3, “2020 Internet Crime Report,” pp. 1–30, 2020.

[8] Makeri, Y. A. “Cyber Security Issues in Nigeria and Challenges,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 4, pp. 315–321, 2017, doi: 10.23956/ijarcsse/v6i12/01204.

[9] David, O. “ICT Use and its Impact in combating Cybercrimes in Abraka , Delta State , Nigeria,” *Res. J. Mass Commun. Inf. Technol. Vol. 3 No. 1 2017 ISSN 2545-529X*, vol. 3, no. 1, pp. 10–23, 2017.

[10] Quayyum, F., Cruzes, D. S., and Jaccheri, L. “Cybersecurity awareness for children: A systematic literature review,” *Int. J. Child-Computer Interact.*, vol. 30, p. 100343, 2021, doi: 10.1016/j.ijcci.2021.100343.

[11] Adesina, S. “Cybercrime and poverty in Nigeria,” *Can. Soc. Sci.*, vol. 13, no. 4, pp. 19–29, 2017, doi: 10.3968/9394.

[12] Chioma, A. “Cybercrime , its Adherent Negative Effects on Nigerian Youths and the Society at Large : Possible Solutions,” *Int. J. Sci. Res.*, no. June, 2020, doi: 10.31695/IJASRE.2019.33658.

[13] Ayinla, M. “The Effect of Adoption of Internet Banking on Performance in the Banking Industry in Nigeria,” *Res. J. Financ. Account. www.iiste.org ISSN*, vol. 9, no. 11, pp. 11–36, 2018, [Online]. Available: www.iiste.org.

[14] Sruthi, “Fraud detection in banking institutions,” *Int. J. Eng. Technol.*, 2016.

[15] Burov, O. “The impact of cybercrime on the digital economy,” *Theory Pract. Intellect. Prop.*, no. 5, pp. 69–78, 2021, doi: 10.33731/52021.244519.

[16] Olarewaju, O. “The impact of cybercrime on the digital economy,” *Theory Pract. Intellect. Prop.*, no. 5, pp. 69–78, 2021, doi: 10.33731/52021.244519.

[17] Ebelogu, C., Samuel, O., Andeh, C., and Agu, E. “Cybercrime, its Adherent Negative Effects on Nigerian Youths and the Society at Large: Possible Solutions,” *Int. J. Adv. Sci. Res. Eng.*, vol. 05, no. 12, pp. 155–164, 2020, doi: 10.31695/ijasre.2019.33658.