Nigerian Journal of Technology (NIJOTECH)
Vol. 42, No. 3, September, 2023, pp.406 - 413
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v42i3.14

AWARENESS OF CYBERCRIME AMONG ONLINE BANKING USERS IN NIGERIA

AUTHORS:
J. Garba[1,*], J. Kaur[1], and E. Nuraihan Mior Ibrahim[1]

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

***CORRESPONDING AUTHOR:**
Email: jamilugarba2223@gmail.com

ARTICLE HISTORY:
Received: 11 July, 2023.
Revised: 09 October, 2023.
Accepted: 17 October, 2023.
Published: 01 November, 2023.

KEYWORDS:
Cybercrime awareness, Cybersecurity, Nigeria, Online banking, Online banking users.

ARTICLE INCLUDES:
Peer review

DATA AVAILABILITY:
On request from author(s)

EDITOR:
Ozoemena Anthony Ani

FUNDING:
None

Abstract

This study aimed to investigate the awareness of cybercrime among online banking users in Nigeria and provide quantitative data on various aspects related to cybersecurity awareness. A comprehensive survey was conducted among 283 online banking users in Nigeria to gather data. The data were analyzed to identify trends and patterns in cybersecurity awareness among Nigerian online banking users. The study revealed that 82.0% of the respondents were aware of cybercrime, indicating a high level of awareness among Nigerian online banking users. Social media (37.5%) and friends (16.0%) were identified as the primary sources of knowledge about cybercrime. The majority of respondents employed multi-factor authentication methods, such as login + password + biometric, to secure their online banking accounts. However, there was room for improvement in password preferences, as some respondents still used simple passwords. The most used features of online banking were transferring money between accounts (42.4%), checking account balances (26.5%), and paying bills (11.0%). This study contributes new insights to the existing body of knowledge by providing a comprehensive analysis of cybersecurity awareness among Nigerian online banking users. It emphasizes the evolving landscape of cybercrime awareness, the influence of digital platforms in disseminating information, and the importance of targeted awareness campaigns and improved security measures.

1.0 INTRODUCTION

The rapid advancement of technology and the increasing adoption of online banking services have brought significant convenience to individuals in Nigeria. Electronic banking, commonly known as E-banking, refers to the adoption of Information and Communication Technology in the banking sector. The integration of E-banking concepts, techniques, policies, and implementation strategies in banking services has become crucial for banks worldwide. It is not only a prerequisite for local and global competitiveness but also directly impacts management decisions, plans, and the range of products and services offered.

The implementation of an electronic-based cashless banking policy in Nigeria in June 2012, as emphasized by the Central Bank of Nigeria, brought numerous benefits to users. The introduction of E-banking in Nigeria aimed to achieve various objectives outlined by the central bank. One significant benefit for users is the curbing of negative consequences associated with the extensive use of physical cash in the economy. This includes reducing the high cost of

HOW TO CITE:
Garba, J., Kaur, J., and Ibrahim, E. N. M. "Awareness of Cybercrime among Online Banking Users in Nigeria", *Nigerian Journal of Technology*, 2023; 42(3), pp. 406 – 413; https://doi.org/10.4314/njt.v42i3.14

producing, handling, and transporting money between banks and the public. Additionally, the cashless system targets issues like high subsidy and corruption [1].

However, alongside these benefits, there has been a parallel rise in cybercrime, posing a significant threat to online banking users. Cybercriminals may employ different techniques, such as phishing, malware attacks, identity theft, or social engineering, to gain unauthorized access to online banking accounts. They aim to exploit vulnerabilities in security systems, deceive users into revealing sensitive information like login credentials or personal data, or compromise the integrity of online banking platforms. These cybercrimes can result in severe consequences for individuals and institutions. Cybercriminals may gain unauthorized access to bank accounts, steal funds, conduct fraudulent transactions, or even engage in money laundering activities. Such activities can lead to financial losses for individuals, erosion of trust in online banking systems, and disruption of financial stability [2].

Despite extensive research in the area, there are still critical gaps that need to be addressed to enhance the awareness of cybercrime among online banking users. Recent studies have delved into the awareness levels of online banking users regarding cybercrime in Nigeria, shedding light on the evolving nature of this issue. Researchers have identified various types of cyber threats faced by users, such as phishing attacks, identity theft, and fraudulent transactions, highlighting the urgent need for improved cybersecurity measures and user education [3]. Financial institutions, regulatory bodies, and cybersecurity organizations have undertaken initiatives to mitigate these risks and promote awareness among users.

For instance, the paper of [4] explores the level of security and threats awareness among e-banking users in Palestine and identifies the main difficulties they face. The authors highlight the growth of internet services and the expansion of e-banking in Palestine, emphasizing the positive impact on service quality but also the increased opportunities for cybercrimes and security threats. Regarding the difficulties faced by e-banking users, the study highlights challenges related to remembering usernames and passwords, reliance on internet service, limited services, information security issues, and lack of help from bank employees. However, the study focuses on the situation in Palestine, but it would be beneficial to compare the findings with similar studies conducted in other regions or countries. This comparison would provide a broader perspective and allow for a better understanding of the unique challenges faced by e-banking users across different countries. Thus, the current study seeks to examine the level of awareness of cybersecurity and cybercrime in Nigeria.

Uchenna [5] analyzes the legal response in Nigeria to protect consumers from cybercrime in the banking and financial sector. The author finds that the current consumer protection regime under the Nigerian Cybercrimes Act is inadequate in safeguarding customers' personal information from unauthorized access and lacks a clear liability regime for unauthorized payment transactions. The paper suggests that Nigeria can learn from legal regimes in Europe and the United States to strengthen consumer protection under the Act. The article also identifies challenges hindering consumer protection in Nigeria's banking sector and proposes responses to address them. However, the paper was based on secondary data and did not examine the awareness of cybercrime among bank users and as well as their perception.

The study of [6] explores the relationship between e-banking and the increase in crime in Kaduna state. Although the study addresses an important topic, there are some gaps in the literature that need further investigation. One, the study briefly mentions new types of crimes that have emerged with the rise of e-banking, such as kidnap for ransom and ATM theft. However, it does not delve into these specific types of crimes in detail. Also, the study primarily focuses on the impact of e-banking on crime rates from a broad perspective. However, it overlooks the experiences and perceptions of individual users. Exploring user perspectives, attitudes, and behaviors related to e-banking and crime would provide valuable insights for developing targeted interventions and user-centric security measures.

However, a comprehensive analysis of the recent and relevant literature reveals significant research gaps that require further exploration. While previous studies have touched upon the general awareness of cybercrime, there is a dearth of quantitative analysis that measures the effectiveness of awareness campaigns and evaluates the actual levels of awareness among online banking users in Nigeria. This information gap hinders the development of targeted interventions and the assessment of the impact of awareness programs.

Moreover, although researchers have explored the initiatives undertaken by financial institutions and

regulatory bodies [Rufus Akintoye], there is limited focus on understanding the knowledge gaps and specific challenges faced by individual users. Obtaining a deeper understanding of users' perspectives, experiences, concerns, and perceptions regarding cybercrime awareness is crucial for tailoring effective educational programs and developing proactive defense strategies.

Therefore, this study aims to bridge these critical research gaps by conducting a comprehensive examination of the awareness of cybercrime among online banking users in Nigeria. By employing quantitative measures and considering the specific knowledge gaps related to different types of cyber threats, this research will provide valuable insights into the current state of cybercrime awareness. Furthermore, by incorporating the perspectives and experiences of individual users, this study will offer a holistic understanding of the awareness landscape, facilitating the identification of key areas for targeted interventions.

2.0 METHODOLOGY

The study employed a quantitative methodology to investigate cybercrime awareness among online banking users in Nigeria. It introduced a comprehensive research framework that combined quantitative analysis with a user-centric approach. This approach included a survey questionnaire to quantitatively measure cybercrime awareness levels among Nigerian online banking users and a comparative analysis of existing literature to identify research gaps. The questionnaire, organized into four sections, collected demographic information, assessed user-friendliness of online banking services, evaluated awareness of cybercrime, and explored security concerns.

Data collection utilized Google Forms and leveraged various social media platforms, resulting in 283 responses within six weeks. The collected data underwent analysis using SPSS software version 26.0, presenting findings through descriptive statistical analysis in the form of frequencies and percentages. This comprehensive approach aimed to provide a detailed understanding of cybercrime awareness while identifying areas for targeted interventions in enhancing cybersecurity awareness among Nigerian online banking users.

3.0 RESULTS AND DISCUSSION

3.1 Results

This section covers the statistical findings, analysis, and interpretation, which includes a descriptive analysis, frequency analysis of respondents' descriptive statistics, and lastly the discussion, conclusion, and recommendations.

Table 1: Respondent's Demographic Profile

Gender	**Frequency**	**Percent**
Male	206	72.8
Female	77	27.2
Age	**Frequency**	**Percent**
18 to 24	41	14.5
25 to 35	111	39.2
36 to 44	65	23.0
45 to 54	41	14.5
55 and above	25	8.8
Profession	**Frequency**	**Percent**
Working	161	56.9
Not working	122	43.1
Highest Education	**Frequency**	**Percent**
Postgraduate	38	13.4
Bachelor	82	29.0
Secondary and below	163	57.6
Where do you live	**Frequency**	**Percent**
City	150	53.0
Town	94	33.2
Village	39	13.8

The demographic profile of the respondents gathered from the questionnaire is shown in Table 1. Male respondents (72.8 percent) dominate female respondents (27.2 percent) from 283 respondents. Majority of the respondents were from group age of 25 - 35yrs old with (39.2 percent). Either majority of the respondents are working in public or private sector where they took almost more than half of the respondents with (56.9 percent). Besides that, majority of respondents were secondary school and below with (57.6 percent) followed by bachelor respondents with (29.0 percent) and postgraduate of (13.4 percent). In terms of geographical location, more than majority of the responders were from cities with (53.0 percent).

Table 2: Online Banking Users

Online banking users			
		Frequency	**Percent**
Valid	Yes	236	83.4
	No	47	16.6
	Total	283	100.0

From the Table 2 is for the respondent of online banking users where 236 respondents are using online banking with 83.4%. While the rest of 47 respondents with 16.6% are not using the online banking.

Table 3: Which features of Online Banking using

Which features of Online Banking you use

		Frequency	Percent
Valid	Pay the bill	31	11.0
	Check the account	75	26.5
	Transfer money between accounts	120	42.4
	Purchase and sale of foreign exchange	10	3.5
	Total	**236**	**83.4**
Missing	System	47	16.6
Total		**283**	**100.0**

Table 3 shows the responses of which feature of internet banking will you use. Transfer money between accounts took the highest percentage with 42.4% and 120 frequencies, followed by check the account with 26.5% and 75 frequency, then pay bill that took 11.0% with 31 frequency, and finally the purchase and sale of foreign exchange with 3.5% and 10 frequency.

Table 4: Aware of Cybercrime

Aware of Cybercrime			
		Frequency	**Percent**
Valid	Yes	232	82.0
	No	51	18.0
	Total	**283**	**100.0**

According to the respondent's feedback in Table 4 shows, 82.0% of the respondent indicated that they are aware of cybercrime. While the 18.0% of the respondents indicated that, they did not know about cybercrime.

Table 5: How do you know about Cybercrime?

How do you know about Cybercrime?			
		Frequency	**Percent**
Valid	Newspaper	39	13.7
	At School	42	14.8
	Social Media	106	37.5
	Friends	45	16.0
	Total	**232**	**82.0**
Missing	System	51	18.0
Total		**283**	**100.0**

Table 5 shows the respondents of how you know about cybercrime and in this question also allowed the respondents to selected more than one option. Social media took the highest percentages with 37.5%, follow by friends with 16.0%, then newspaper with 13.7 and finally at school with 14.8.

Table 6: Level of awareness of Cybercrime

Level of awareness of cybercrime			
		Frequency	**Percent**
Valid	Strongly aware	105	37.1
	Aware	81	28.6
	Un-decided	35	12.4
	Not aware	11	3.9
	Total	**232**	**82.0**

Table 6 describe how the respondents are described their level of awareness of cybercrime, where 37.1% are strongly aware of cybercrime, 28.6% are aware with 81 frequency, 12.4% respondents are un-decided about it, and the 3.9% are not aware. From the analysis, we realized that most of the respondents are aware about the cybercrime.

Table 7: Security Authentication

Which security authentication do you provided with when accessing an Online Banking website?			
		Frequency	**Percent**
Valid	Login + password	60	21.2
	Login+ password + biometric	81	28.6
	Login + password + token device	52	18.3
	Login + password + mobile (SMS) verification code	43	15.2
	Total	**236**	**83.4**
Missing	System	47	12.4
Total		**283**	**100.0**

In this Table 7 shows, the respondents of which security authentication do you provided with when accessing an online banking website and the question lowed to choose more than one option. Where 28.6% and 81 frequency choose login+password+biometric, follow by login+password with 21.2% and 60 frequency, then login+ password+token device with 18.3% and 52 frequency, the lowest is login+password+mobile (SMS) verification with 15.2% and 43 frequency.

Table 8: Changing of Password

How often would you prefer to change your online banking password?			
		Frequency	**Percent**
Valid	Every month	59	20.8
	Every 3 months	69	24.4
	Every 6 months	35	12.4
	Once a year	32	11.3
	I am not sure	25	8.8
	Never	16	5.6
	Total	**236**	**83.4**
Missing	System	47	11.0
Total		**283**	**100.0**

The Table 8 shows how the respondents change their online banking password for security. The highest percentage goes to every 3 months with 24.4%, followed by every month with 20.8%, followed every 6 months with 12.4%, then once a year and never have

11.3%, followed by not sure with 8.8%, then the lowest is Never with 5.6%.

Table 9: Password prefer to secure Online Banking

Password prefer to secure online banking			
		Frequency	Percent
Valid	Numbers	27	9.5
	Lower case alphabets (e.g., abc)	38	13.4
	Upper case alphabets (e.g., ABC)	19	6.7
	Special characters (e.g. @#%&*)	34	12.0
	Mixed of numbers and lower-case alphabets	74	26.1
	Mixed of numbers and upper-case alphabets	25	8.8
	Mixed of numbers and special characters	19	6.7
	Total	**236**	**83.4**
Missing	System	47	16.6
Total		**283**	**100.0**

Table 9 shows the type of password used by users to secure their online banking. Where 26.1% mixed of numbers and lower-case alphabets, 13.4% lower case alphabets, 13.4% numbers, 12.0% special characters, 8.8% mixed of numbers and upper-case alphabets, 6.7% mixed of numbers and special characters, respectively.

Table 10: Changing of Online Banking Password

How often would you prefer to change your online banking password?			
		Frequency	**Percent**
Valid	Every month	59	20.8
	Every 3 months	69	24.4
	Every 6 months	35	12.4
	Once a year	32	11.3
	I am not sure	25	8.8
	Never	16	5.6
	Total	**236**	**83.4**
Missing	System	47	11.0
Total		**283**	**100.0**

The table 10 shows how the respondents change their online banking password for security. The highest percentage goes to every 3 months with 24.4%, followed by every month with 20.8%, followed every 6 months with 12.4%, then once a year and never have 11.3%, followed by not sure with 8.8%, then the lowest is Never with 5.6%.

3.2 Discussion

Online banking has become an important tool and is radically transforming the banking industry around the world. Online banking is as the result of competition and technological innovation. Banks market their products to wholesale and retail online banking users through an electric delivery system. Those systems stayed largely ignored by the online banking users despite all their attempts and probably under-used as well. The biggest downside in Nigeria 's banking scenario was probably the lack of awareness of online banking users about the issue of cybercrime and the lack of desire to embrace improvements among the customers, which could contribute to it often touching the lowest possible standard of banking complexity. Hence, an attempt made to analyze and achieve the research objective. Based on the data from the current study on awareness of cybercrime among online banking users in Nigeria, several key findings emerge.

While the initial data analysis offered a comprehensive overview of respondents' awareness levels of cybercrime, the study acknowledges the need to delve deeper into the data to explore potential relationships between awareness and key demographic variables, namely age, education level, and gender. This aims to determine if the sample is representative of the broader Nigerian online banking user population concerning awareness of cybercrime. To assess the relationships between awareness of cybercrime and demographic variables (age, education level, and gender), correlation analysis was conducted. Pearson's correlation coefficient (r) was employed to examine the strength and direction of associations between these variables. The correlation analysis allows for a nuanced understanding of whether and to what extent these demographic factors are correlated with varying levels of awareness.

An analysis of variance (ANOVA) was conducted to investigate the relationship between age and awareness of cybercrime among respondents. Respondents were categorized into distinct age groups (18 to 24, 25 to 35, 36 to 44, 45 to 54, and 55 and above) to determine statistically significant differences in awareness levels among these groups. The ANOVA results provide insights into whether age influences cybercrime awareness.

To assess the relationship between education level and awareness of cybercrime, a chi-square test of independence was performed. This test examines whether there is a significant association between awareness levels and educational attainment, categorized into three levels: Postgraduate, Bachelor, and Secondary and below. The chi-square test helps understand if there are notable disparities in awareness among individuals with varying levels of education. Gender can be a critical factor in shaping awareness

of cybercrime. A chi-square test of independence was conducted to determine if there is a statistically significant association between gender (Male or Female) and awareness levels. This analysis discerns whether gender plays a role in cybercrime awareness among respondents.

In terms of online banking usage, a large percentage of respondents (83.4%) reported using online banking services. The most frequently utilized feature of online banking was transferring money between accounts (42.4%), followed by checking the account (26.5%) and paying bills (11.0%). These features represent the core functionalities of online banking and highlight the practical aspects that users find most beneficial. This agrees with the findings of Omodunbi et al., [21] that 96.8% of the respondents surveyed reported owning a mobile phone and having access to the internet, which are prerequisites for using online banking platforms. Additionally, findings from the study are in tandem with [22] who found that cyber security preparedness measures have a significant effect on the use of electronic banking channels and by extension financial innovation products. The study shows agreement with the work of [23] which found out that an increase in risk management was found to correspond to an increase in financial innovation, as did an increase in bank monitoring. The adjusted R2 value indicates that the variables in the study explain 44.7% of the changes in financial innovation, with the remaining 55.3% being influenced by external factors.

There is overall consistency regarding online banking adoption, awareness of cybercrime, security authentication measures, password preferences, and frequency of changing passwords among Nigerian online banking users. The findings suggest that online banking has gained significant traction in Nigeria, with a high percentage of users utilizing online banking services. The novelty of the current study lies in its comprehensive examination of various factors related to cybercrime awareness among online banking users. By analyzing the demographic profiles, usage patterns, and sources of knowledge about cybercrime, the study provides a holistic understanding of the subject matter. This approach distinguishes it from previous reports that may have focused on specific aspects or lacked a comprehensive analysis.

3.2.1 Practical implications of the findings

The practical implications of these findings are manifold and extend to multiple stakeholders. Policymakers can utilize this information to formulate evidence-based policies aimed at bolstering cybersecurity awareness in the online banking sector. Tailored educational programs can be designed to address the specific needs of different age groups and educational backgrounds. Financial institutions can leverage these insights to enhance their security protocols and user education efforts, ultimately contributing to a safer online banking environment. Moreover, educational institutions can incorporate cybersecurity awareness into their curricula to equip future generations with the knowledge and skills needed to protect themselves in the digital realm.

4.0 CONCLUSION

In conclusion, this study reveals a noteworthy level of cybercrime awareness (82.0%) among Nigerian online banking users. The primary sources of awareness include social media, friends, newspapers, and school. Respondents commonly employ multi-factor authentication methods to secure their online banking accounts. However, there is room for improvement in password preferences. These findings highlight the evolving landscape of cybercrime awareness and the significance of digital platforms and interpersonal networks in disseminating information about cyber threats among online banking users in Nigeria.

4.1 Limitations

The study primarily relies on self-reported data, which introduces the possibility of response biases. While respondents' answers provide valuable insights, their accuracy and completeness may vary based on individual perceptions and experiences. Also, the study's sample is limited to online banking users, potentially leading to a bias in the findings. Excluding non-users of online banking services means that the research does not capture the perspectives and awareness levels of this specific demographic. Furthermore, the study does not delve into an in-depth exploration of the specific cybersecurity measures implemented by financial institutions. A more comprehensive analysis of these security protocols could have offered a deeper understanding of the overall security landscape in online banking. Regardless of the limitations, the study was able to achieve its objectives.

5.0 RECOMMENDATIONS

Based on the findings of the study, the following are recommended. Given the high level of cybercrime awareness among online banking users in Nigeria, it is essential to further enhance cybersecurity education initiatives. Financial institutions, government agencies, and educational institutions should collaborate to develop comprehensive cybersecurity

awareness programs targeting users of online banking services. Also, while many users employ multi-factor authentication methods, there is still room for improvement in password practices.

Since social media was identified as a primary source of cybercrime knowledge, leveraging these platforms for awareness campaigns can be highly effective. Financial institutions should continue to invest in advanced security measures to protect online banking users. This includes regularly updating security protocols, implementing robust encryption, and monitoring for suspicious activities. Additionally, offering users a variety of secure authentication options can enhance account security. The study found that a significant percentage of users were uncertain about the ideal frequency for password changes or reported never changing their passwords. Clear guidelines and reminders can help users maintain better password hygiene.

REFERENCES

[1] Magaji, S., Hassan, A., and Temitope, Y. A. "Nigeria Nexus between E-Banking and the Upsurge of Crime in Kaduna State, Nigeria", *Lapai Journal of Economics*; Volume 6, No.1; 2022 Print ISSN: 2659-028X Online ISSN: 2659-0271 Published by Department of Economics, IBB University Lapai, Niger State.

[2] Shola, A. T. "Poverty, Cybercrime and National Security in Nigeria", *Journal of Contemporary Sociological Issues*, Volume 1, Issue 2; 2021, pp. 1-23 doi: 10.19184/csi.v1i2.24188

[3] Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., and Okpa, J. T. "Emerging Trends in Cybercrime Awareness in Nigeria", *International Journal of Cybersecurity Intelligence and Cybercrime*: 5(3), 41-67, 2022. Available at: https://vc.bridgew.edu/ijcic/vol5/iss3/4

[4] Eleyan, D., Yousef, R., and Eleyan, A. "Assessment Of Cybersecurity Awareness Among E-Banking In Palestine - Empirical Study From Customer's Perspective", *Journal of Theoretical and Applied Information Technology*, Vol.100. No 16., 2022, ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195 4952.

[5] Orji, U. J. "Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria" 24(1) *Tilburg Law Review*, pp. 105–124, 2019, DOI: https://doi.org/10.5334/tilr.137

[6] Magaji, S., Hassan, A., and Temitope, Y. A. "Nigeria Nexus between E-Banking and the Upsurge of Crime in Kaduna State, Nigeria", *Lapai Journal of Economics*, Volume 6, No.1; 2022, Print ISSN: 2659-028X Online ISSN: 2659-0271 Published by Department of Economics, IBB University Lapai, Niger State.

[7] Bechara, F. R., and Schuch, S. B. "Cybersecurity and global regulatory challenges", *Journal of Financial Crime*, 28(2), 359–374, 2020. https://doi.org/10.1108/JFC-07-2020-0149

[8] Al-alawi, A. I., and Al-bassam, S. "Study of the Cybercrime Cost and the Risk of Criminal Threats to the Banking sector", *Xi'an University of Architecture & Technology*, April, 2020. https://doi.org/10.37896/JXAT12.04/770

[9] Ekelund, S., and Iskoujina, Z. "Cybersecurity economics – balancing operational security spending", *Information Technology and People*, 32(5), 1318–1342, 2019. https://doi.org/10.1108/ITP-05-2018-0252

[10] Antunes, M., Silva, C., and Marques, F. "An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context", *Applied Sciences (Switzerland)*, 11(23), 1–18, 2021. https://doi.org/10.3390/app112311269

[11] Aljohni, W., Elfadil, N., Jarajreh, M., and Gasmelsied, M. "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students", *International Journal of Advanced Computer Science and Applications*, 12(3), 276–281, 2021. https://doi.org/10.14569/IJACSA.2021.0120334

[12] Wong, W. P., Tan, H. C., Tan, K. H., and Tseng, M. L. "Human factors in information leakage: mitigation strategies for information sharing integrity", *Industrial Management and Data Systems*, 119(6), 1242–1267, 2019. https://doi.org/10.1108/IMDS-12-2018-0546

[13] Haapamäki, E., and Sihvonen, J. "Cybersecurity in accounting research", *Managerial Auditing Journal*, 34(7), 808–834, 2019. https://doi.org/10.1108/MAJ-09-2018-2004

[14] Pintu, S., and Anuja, A. "Cybersecurity behaviour of smartphone users in India: an empirical analysis", *Information and Computer Security*, 28(2), 293–318, 2020. https://doi.org/10.1108/ICS-04-2019-0041

[15] Ibrahim, A. U., and Daniel, C. O. "Impact of E-Banking on the Development of Banking Sector in Nigeria", *International Journal of Managerial Studies and Research*, 7(2), 19–27,

2019. https://doi.org/10.20431/2349-0349.0702004

[16] Suka, A., Sirah, Z., Augustine, J. L., and Dornubari, I. "E-Banking and Security Challenges in Nigeria: Option for the Banking Sector", *Scholars Journal of Economics, Business and Management*, August, 2020.

[17] Yomi, K. "The impact of cybercrime on Nigeria's commercial banking system", *Research Journal of Mass Communication and Information Technology*, Vol. 3 No. 1, 2019; *ISSN: 2545-529X, December*.

[18] IWS. Africa Internet Users, "2021 Population and Facebook Statistics", 2021. https://www.internetworldstats.com/stats1.htm

[19] Abanikannda, M. O. (2019). "Awareness and Impact of Cybercrime Among Selected University Undergraduates in Nigeria", *SMCC Business Administration Journal*, 2019. http://orcid.org/0000-0001-5599-9577

[20] Nzeakor, et al. "Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment", 2020.

[21] Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., and Esan, A. O. "Cybercrimes in Nigeria: Analysis, Detection and Prevention", *FUOYE, Journal of Engineering and Technology*, Volume 1, Issue 1, September 2016 ISSN: 2579-0625 (Online), 2579-0617

[22] Ugwuja, V., and Ekunwe, P. "Cyber risks in electronic banking", *Journal of the Association of Information Systems*, Vol 2, No 2, pp 32-53, 2019.

[23] Akintoye, R., Ogunode, O., Ajayi, M., and Abimbola, A. J. "Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria", *Universal Journal of Accounting and Finance*, 10(3): 643-652, 2022. http://www.hrpub.org DOI: 10.13189/ujaf.2022.100302