JLSTAN, VOLUME 1, ISSUE 1, 2024

Cybercrime Impact on Stem Students' Educational Trajectories: Family Accounts as Vulnerable Targets

Imran A. Adeleke & Fatimah Y. Akinrinola

Department of Computer Science Education, College of Information and Technology Education

Lagos State University of Education, Lagos, Nigeria.

KEYWORDS:

cybercrime, family accounts, STEM students, interest, and educational pursuit.

WORD COUNT:
164

CORRESPONDING EMAIL ADDRESS:

adelekeai@lasued.edu.ng

ABSTRACT

This study examined the impact of cybercrime on family accounts and its implications for STEM students' educational pursuits. Two research questions and corresponding hypotheses were formulated to provide deeper insights into the study. Using a descriptive survey design, data were collected through an online Google Form questionnaire. A total of 73 students were conveniently sampled from a Lagos State University of Education. Data were analyzed using frequency tables and chi-square. The findings revealed a significant impact of cybercrime on family accounts ($\chi 2 = 44.745$, $p < 0.05$) and a significant effect of cybercrime on STEM students' interest in their academic pursuits ($\chi 2 = 47.499$, $p < 0.05$). Based on these findings, it is recommended that families undergo orientation sessions and recognize cybercrime as a serious offense that not only jeopardizes individual and family security but also impacts broader societal dynamics. Building awareness about cybersecurity measures and promoting confidentiality within family financial discussions could mitigate the negative impact of cybercrime on STEM students' educational aspirations.

HOW TO CITE

Adeleke I.A & Akinrinola F.Y. (2024). Cybercrime Impact on Stem Students' Educational Trajectories: Family Accounts as Vulnerable Targets. JSTAN, 1(1), pg 22-32.

Introduction

The world economy is experiencing swift changes and increased availability of information technology (IT) since the 1980s, its incorporation has become an indispensable aspect of our daily lives, yielding significant social and economic impacts (Clemons et al., 2017). The digital revolution plays an important role in the economy driven by information, facilitating easy access to information, and thereby transforming our patterns of interaction and social engagement (Baller et al, 2016). This shift promotes notions of equality and democracy. Nevertheless, the digital revolution presents a dual facet, offering substantial opportunities alongside notable threats to societies, economies, and national security (Świątkowska, 2020). Criminals have adapted their tactics to exploit vulnerabilities in cyberspace, leading to an ever-evolving landscape of cyber threats (Baller et al, 2016). Cybercrimes have manifested in different forms ranging from mild instances of unauthorized access to the dissemination of disinformation through digital communication channels, online fraud, scams, and illicit trade, as well as various forms of organized crime, attacks on critical infrastructure with the intent of causing substantial disruption, political and industrial espionage, and coordinated terrorist activities facilitated through the internet (Świątkowska, 2020). Other unsuspected actors negatively influencing the cyberspace include nation-state actors, cyber terrorists, hacktivists, and trolls (Pawlicka et al. 2020; Stoddart, 2022).

Świątkowska (2020) explained that the escalation of cybercrime can be attributed to various factors, among which scalability is a key driver. This scalability is often associated with diverse factors such as advancements in technology and automation. In addition, Cybercrime is characterized by its cost-effectiveness, high profitability, and growing simplicity in execution. The emergence of cyberattacks-as-a-service, facilitated by illicit marketplaces within the Darknet, plays a significant role in providing easy access to tools for potential perpetrators, allowing them to engage in cybercrimes even without extensive technical expertise. Offenders can easily procure the essential tools and tutorials online, eliminating the need for sophisticated knowledge or skills to carry out illicit activities. Therefore, the cyberspace is a battleground, where individuals, organizations, or even entire states can become targets of malicious hackers or unscrupulous cybercriminals (Pawlicka et al. 2020).

Literature documents several cases of cyber-attacks to organisations. For example, Nurse and Bada (2019), noted the instances of cyber assaults directed at the FBI, the US Department of Justice, and the US Copyright Office, including declarations of war targeting banks and stock exchange markets. Additionally, notable cybercriminal groups such as LizardSquad, known for disrupting Sony's PlayStation Network and causing a flight disruption with a bomb scare, and the hacker group Lulzsec, which pilfered private data from 24.6 million customers through a hack on Sony's PlayStation Network, have gained notoriety. While cybercriminals might function as decentralized networks, available evidence (Piasecki et al. 2021) indicates that their members tend to be in close geographic proximity, even in cross-national attacks. Notably, small local networks and groups formed around relatives and friends continue to play substantial roles in these activities (Nurse & Bada, 2019).

In Nigeria, cases of cyber- attacks have been attributed to youths. Cybercrime in Nigeria is increasingly appealing to Nigerian youths as a means to attain wealth and elevate their social status (Ukam et al., 2024). Unlike traditional crimes such as armed robbery, cybercrime offers perceived safety and security, often conducted from the comfort of one's

home. Adaramola (2024) reports on the Nigeria Inter-Bank Settlement (NIBBS) indicated that there were approximately 46,126 attempted attacks by fraudsters in the first nine months of 2020, with 41,979 of these attempts proving successful, reflecting a 91% success rate. During the same period, the banking sector in Nigeria incurred losses exceeding five billion Naira due to internet fraud (Egboboh, 2021). The escalating concerns surrounding cybercrime in Nigeria have led some to describe it as reaching epidemic proportions.

However, the resulting effect of cybercrime cannot be overemphasized. The risk is particularly evident in the least developed countries, where the surge in internet usage has not been accompanied by corresponding educational efforts (Howell, 2016). In the digital age, where technology intertwines seamlessly with education, the impact of cybercrime extends beyond financial losses and data breaches. Victims often experience financial loss, identify theft, emotional distress, and stress and guilt. In addition Obinna et al. (2022) discovered that the distinctive nature of cybercrime lies in the voluntary involvement of its victims, who unwittingly immerse themselves in it without coercion. Initially appearing as innocuous interactions, such as friendly conversations and cordial exchanges, these interactions swiftly transition into a series of fraudulent activities. Consequently, victims find themselves emotionally and mentally distressed, often resorting to irrational behavior before law enforcement intervenes to apprehend the perpetrator(s).

The Science, Technology, Engineering, and Mathematics (STEM) field is integral to the global workforce. Numerous nations worldwide, Nigeria included, depend on STEM disciplines to secure a foothold in the global economy. The Nigerian government actively pursues solutions to economic development and self-sufficiency, recognizing the pivotal role of STEM Education in maximizing potential. This strategic focus aims to cultivate a competitive future workforce equipped with essential 21st-century skills (Matazu, 2021). Understanding the challenges posed by cyber threats to the educational journeys of aspiring STEM professionals is crucial. Without protective measures, any family is susceptible to cybercrime which could adversely impact the educational journey of students whose family is affected by cybersecurity breaches. However, the emphasis on STEM students is due to the critical role STEM plays in driving economic development in the fourth industrial revolution. Any detrimental effects on future students within STEM fields could significantly impact the economy as a whole. This study therefore seeks to explore a specific and often overlooked aspect – the repercussions of cybercrime on the educational trajectories of STEM students, with a particular focus on the vulnerability of family accounts. This study therefore asks two questions: (i) will cybercrime attacks have impact on STEM students' family accounts? and (ii) to what extent have cybercrime attacks experienced by STEM students affected their interest in academic pursuits?

Statement of the Problem

As digital technologies increasingly integrate into educational practices, the utilization of family accounts for accessing resources and fostering collaborative learning environments has become widespread. Recently, a large scale of cybercrime have been reported (Adaramola, 2023) and the pervasive menace of cybercrime presents considerable obstacles, as family accounts emerge as prime targets for malicious individuals aiming to exploit vulnerabilities and compromise sensitive data. Despite the growing acknowledgment of cyber threats directed at family accounts among Nigerian citizens, there exists a gap in comprehending the impact of cybercrime on STEM students' educational

endeavors through assaults on family accounts, as well as its encompassing potential disruptions to learning activities, psychological effects and implications for academic achievements and career aspirations.

Purpose of the study

The purpose of this study is to explore the impact of cybercrime on STEM students' educational trajectories through vulnerable family accounts.

Research hypotheses

HO_1: Cybercrime does not have a significant impact on the family accounts of STEM students.

HO_2: Cyber threats faced by STEM students through attacks on family accounts do not influence their attitudes towards academic pursuits.

Study Significance

Focusing specifically on STEM students, this study offers valuable insights into the impact of cybercrime on individuals pursuing careers in vital fields within today's digital era. The research aims to provide empirical evidence regarding the financial consequences of cyber-attacks on families within this academic community. Moreover, the study intends to illuminate the intersection of cybersecurity concerns with students' attitudes, particularly their academic motivation and engagement. This understanding can guide the development of supportive environments and resources tailored to assist STEM students in navigating challenges and maintaining their focus on academic pursuits. Furthermore, the findings of this study have the potential to inform strategies aimed at bolstering resilience and coping mechanisms among STEM students. Such initiatives are crucial to ensuring that cyber threats do not undermine their enthusiasm for learning and pursuit of knowledge. Through rigorous testing of these hypotheses, researchers aim to deepen our understanding of the multifaceted impacts of cybercrime on family accounts, academic attitudes, and interests within the STEM community. Ultimately, the insights generated by this research can inform targeted interventions, policies, and support mechanisms designed to mitigate the adverse effects of cyber threats and foster resilience among STEM students.

Review of Related Literature: Concept of Cybercrime

The concept of cybercrime encompasses a broad range of illicit activities perpetrated through digital technologies and the internet. Unlike traditional forms of crime, cybercrime transcends geographical boundaries and often exploits the anonymity and interconnectedness of the online world to perpetrate various malicious acts (Al-Hakimi & Nur, 2023). From financial fraud and identity theft to hacking and malware attacks, cybercriminals employ sophisticated techniques to exploit vulnerabilities in computer systems, networks, and digital infrastructure. The advent of cyberspace has not only revolutionized the way individuals communicate, conduct business, and access information but has also introduced new avenues for criminal exploitation.

Cybercrime includes unlawful actions carried out on or by means of a computer such as internet fraud or use of computer to commit numerous crimes such as email scams- to cheat unsuspecting people, hacking- by people who create viruses intentionally to gain access and harm computer data, while others introduce worms to destroy computer data, stealing data, people's identity, obtaining funds under false pretense known as (419), and introducing malicious traffic from many sources to make real services unavailable to company server (Adenusi et al. 2020).

Crime appears to be a permanent feature of the modern society. Despite efforts of social workers, law enforcement agency, personal and criminal

justice professionals to minimize it, the world is becoming a more terrible place. Cybercriminals, hackers, and spammers exert a significant influence over the internet, preying on unsuspecting users and subjecting them to various forms of exploitation. Their activities often involve abuse, blackmail, and the illicit trade of personal information, leading to devastating consequences for victims. Instances of severe abuse, manipulation, and fear induced by cybercriminal tactics can result in tragic outcomes such as suicide (Al-Hakimi & Nur, 2023). Beyond the direct financial and operational impacts, cybercrime can also have far-reaching consequences for individuals, businesses, and society at large, eroding trust in online systems, compromising personal privacy, and undermining the integrity of critical infrastructure.

The concept of cybercrime underscores the need for comprehensive strategies to address the multifaceted challenges posed by digital threats. This includes enhancing cybersecurity measures, promoting digital literacy and awareness, fostering international cooperation, and enacting robust legal frameworks to deter cybercriminal activity and hold perpetrators accountable.

Family financial account and cybercrime

In the modern era of digital technology, the widespread availability of online platforms and services has fundamentally altered the landscape of cybercrime, presenting unprecedented challenges for both individuals and families alike. As the number of interconnected devices continues to rise and digital transactions become increasingly common, the looming threat of cyber-attacks casts a shadow over households worldwide (Ayub & Akor, 2020). While family accounts offer convenience and efficiency in managing digital assets they also present lucrative opportunities for cybercriminals seeking to exploit vulnerabilities (Jain et al., 2021). This therefore has effect on the victims and their family at large. For example, Button et al. (2021) identified from their study some of the impact of cybercrime on accounts. The researchers identified financial loss and fear among others. Kakineen et al. (2018) also suggest that, similar to experiencing victimization in the physical world, being a victim of cybercrime is a detrimental experience, particularly for individuals with limited social support offline to help them cope with the resulting stressors. Whether through targeted phishing schemes aimed at shared email accounts or sophisticated ransomware attacks targeting family cloud storage, the risks associated with family accounts underscore the urgent need for heightened awareness and proactive cybersecurity measures. Navigating the complexities of the digital realm requires families to cultivate a culture of vigilance, resilience, and collaboration, thereby mitigating the impact of cybercrime and safeguarding the integrity of their digital holdings.

Family Account and Cybercrime impact on STEM students' interest in educational pursuit

The effects of cybercrime on family accounts have a ripple effect on STEM students' interest in their educational pursuits (Edidiong et al., 2023). Family accounts, designed to streamline digital asset management and foster collaborative interactions within households, become vulnerable targets for cybercriminal exploitation. Instances of data breaches, identity theft, or financial fraud perpetrated through compromised family accounts can disrupt the trust and security within familial environments, leading to heightened anxieties and concerns among STEM students (Rao et al. 2023). As aspiring scientists, technologists, engineers, and mathematicians, STEM students heavily rely on digital tools, online resources, and collaborative platforms to access information, conduct research, and engage in hands-on learning experiences (Fang et al., 2021). The compromised integrity of family

accounts may also impact students' access to essential educational resources, hindering their ability to engage effectively in learning activities and collaborative projects. However, (Berozashvili, 2024) noted that recovering from cybercrime effects can be a lengthy and distressing process for individuals, often involving complicated legal procedures and the possibility of enduring long-term financial and psychological consequences. Therefore, the fear of falling victim to cyber threats may therefore deter STEM students from fully embracing digital technologies or participating in collaborative online initiatives, thereby impeding their interest. Moreover, the pervasiveness of cyber threats within familial settings underscores the importance of digital literacy and cybersecurity education for STEM students, empowering them to navigate online risks and protect their personal and academic interests.

Theoretical Framework

The Routine Activity Theory, developed by Cohen and Felson (1979), suggests that crime is a result of the convergence of three factors: a motivated offender, a suitable target, and the absence of a capable guardian. In the context of cybercrime, this theory implies that the presence of vulnerable systems (suitable targets), motivated cybercriminals, and a lack of effective cybersecurity measures (absence of capable guardians) creates opportunities for cybercrime to occur. When applied to this study, this theory suggests that cybercriminals, motivated by various factors such as financial gain or personal vendettas, exploit vulnerabilities in family accounts, which serve as suitable targets (DeLiema, 2017). However, STEM students, whose educational pursuits heavily rely on access to technology and the internet, the compromise of family accounts due to cybercrime can have significant consequences. For example, if a family's financial accounts or personal information are compromised, it can lead to disruptions in the student's educational pursuits, including difficulties in accessing necessary resources for learning, such as educational software, online resources, or even tuition payments. Furthermore, the absence of capable guardianship in the form of robust cybersecurity measures exacerbates the vulnerability of family accounts to cybercrime. Without adequate protection, such as strong passwords, regular software updates, and awareness of phishing attempts, family accounts remain easy targets for cybercriminals.

Routine Activity Theory helps to explain how the convergence of motivated offenders, vulnerable targets (family accounts), and the absence of capable guardianship (lack of effective cybersecurity measures) contributes to the impact of cybercrime on STEM students' educational trajectories. Understanding these dynamics is crucial for developing effective strategies to mitigate the negative effects of cybercrime and safeguard the educational pursuits of STEM students.

Method

Research Design

This study employed a descriptive survey design. The utilization of a descriptive survey design in this study was chosen due to its capacity to gather extensive information relevant to the study's objectives.

Study Population

The study population comprises students of a University in Lagos state Nigeria. The total population of students are three hundred and eighty nine (389) students.

Sample and Sampling Techniques

Convenience sampling technique was used and the study's sample comprised full-time STEM students in a Lagos State University. The choice of

convenience sampling was due to the availability and easy access of the students who participated in the study. Seventy (74) students, comprising Computer Science (86.5%) and Biology (13.5%) were sampled from the population.

Research Instrument

The primary tool utilized for data collected was a self-designed questionnaire named cybercrime and family account questionnaire (CFAQ). This questionnaire comprised two sections: Section A gathered demographic information from respondents, while Section B addressed the variables outlined in the hypotheses using four likert scale format such as "Strongly Agree" (SA), "Agree" (A), "Disagree" (D), and "Strongly Disagree" (SD); and Very large extent (VLE), large extent (LE), very low extent (VLE), low extent (LE) to indicate their responses. The instrument was designed by the researchers using Google Form.

Data Collection and Analysis

Data was collected through Google Form. The link was sent to the student's WhatsApp platform to fill, and this was opened for one week before the submission of responses were stopped. The Google form was linked to a Google sheet for data collation. The collated data were arranged and analysed using mean rating whose decision mean is 2.50, and chi-square tests. Data were analysed using Statistical Package for the Social Sciences (SPSS version 21).

Validation and Reliability of the Instrument

To ensure the validity of the instrument, a preliminary version of the questionnaire was provided to experts in the field to evaluate its construct and content validity. After incorporating their feedback, revised versions of the instrument were pilot-tested. The reliability coefficient index obtained from this pilot test was 0.87, indicating a high level of reliability for the study.

Results

This section presents the results of the findings based on the data collected.

Research question 1: Will cybercrime attacks have impact on STEM students' family accounts?

Table 1: Cybercrime impact on family accounts

S/N	STATEMENT	SA	A	D	SD	Mean
1.	The severity of cybercrime does not affect families.	2	17	15	37	1.77
2.	Cybercrime led to loss of money in our family account	15	40	13	3	2.32
3.	Cybercrime cause family dispute over the loss of money in my family account	20	41	9	2	3.10
4.	Individuals/family members are cybercrime perpetrators of family account	7	36	26	5	2.61
5.	Family accounts are prone to cybercrime attacks because of lack of secrecy of information among account owners.	21	36	11	2	3.09
6.	My family has experienced a cybercrime incident (e.g., identity theft, financial fraud, phishing scams)?	6	32	25	9	2.49
7.	Based on my experience, Cybercrime affects the financial stability of families?	21	46	4	2	3.24
8.	I have personally experienced financial losses due to cybercrime?	11	27	23	10	2.55

9.	Cybercrime has a significant impact on the family accounts of STEM students?	12	44	13	3	2.90
10.	Families are not equipped to mitigate the impact of cybercrime on their accounts?	9	46	14	2	2.90
Decision Mean = 2.50				**Cumulative Mean 2.70**		

Table 1 above presents mean rating on the impact of cybercrime on STEM student's family accounts. The cumulative mean (2.70), representing the average scores across all and response categories, is higher than the decision mean (2.50). This suggests that cybercrime has an impact on the STEM student's family accounts. However, the mean ratings of items 1(1.77), 4(2.61) and 6(2.49) revealed a low data compared to other responses, suggesting that a few of the students may not have been a victim or affected by cybercrime attacks. Further analysis is presented in the table below.

Hypothesis one: Cybercrime does not have a significant impact on the family accounts of STEM students.

Table 2: Chi-Square Tests on Cybercrime impact on STEM students family accounts

	Value	Df	Asymp. Sig.
Chi-Square	44.745[a]	2	.000
N of Valid Cases	71		

Further analysis revealed on Table 2 that the chi-square (χ^2) statistic is approximately 44.745, the p-value is approximately .000, and the degrees of freedom is 2. Since the $p<0.05$, we therefore reject the null hypothesis, and the result is significant. This indicates that there is a statistically significant relationship between cybercrime and its impact on STEM students' family accounts ($\chi^2 = 44.745$, $p<0.05$).

Research question 2: To what extent have cybercrime attacks experienced by STEM students affected their interest in academic pursuits?

Table 3: Cybercrime effect on STEM students' interest on academic pursuit

S/N	STATEMENT	VHE	HE	LE	VLE	Mean
1	To what extent are you interested in your academic subjects within the STEM field?	31	36	3	1	3.37
2	My parents found it difficult to provide reading materials for me due to them being a victim of cybercrime.	4	14	36	17	2.31
3	To what extent have you experienced any changes in your academic performance in STEM subjects as a result of concerns about cybercrime affecting your family's accounts?	8	20	29	14	2.07
4	To what extent has Cybercrime negatively influence your academic success in different STEM subjects?	3	22	33	12	2.23

5	How do you balance your interest in pursuing academic goals within the STEM field with concerns about cybercrime affecting your family's accounts?	12	31	21	6	2.70
6	To what extent has your experience with Cybercrime on your family's account affected your academic motivation within STEM field?	10	21	21	19	2.31
7	I have considered pursuing further education or career opportunities within STEM field based on my level of interest despite the effect of cybercrime on my family?	20	32	13	6	2.93
Decision Mean = 2.50					**Cumulative Mean 2.56**	

Table 3 above presents the mean rating on the extent of the impact of cybercrime on STEM student's interest in their education. The cumulative mean (2.56), representing the average scores across all and response categories, is slightly higher than the decision mean (2.50). This suggests that cybercrime has an impact on the STEM student's family accounts but not to a great extent. This is evident in the mean rating of item 2(2.31), 3(2.07), 4(2.23), 6(2.31). Further analysis on the data is presented below.

Hypotheses 2: Cybercrime attacks experienced by STEM students through attacks on family accounts does not significantly affect their interest in academic pursuits.

Table 4: Chi-Square Tests on Cybercrime attacks on STEM students interest on academic pursuit

	Value	**df**	**Asymp. Sig.**
Chi-Square	47.499a	3	.000
N of Valid Cases	71		
	Value	df	Asymp. Sig.

Results from Table 4 revealed that the chi-square (χ^2) statistic is approximately 47.499, the p-value is approximately .000, and the degrees of freedom is 3. Since the $p<0.05$, we therefore reject the null hypothesis, and the result is significant. This indicates that there is a statistically significant association between cybercrime attacks experienced by STEM students' and their interest on their academic pursuit ($\chi^2 = 47.499$, $p<0.05$).

Discussion of findings

This study investigated the effect of cybercrime attacks on family account and how it influences STEM student's educational trajectories. Two hypotheses were stated and findings revealed that the two null hypotheses were rejected. First, findings revealed a significant

association between cybercrime and family accounts among STEM students ($\chi^2 = 44.745$, $p<0.05$). This finding aligns with previous research and supports the routine activity theory (Cohen & Felson, 1979) emphasizing the vulnerability of family accounts to cyber threats (Jain, et al, 2021). Cybercriminals often target family accounts due to their potential access to sensitive information and resources shared among household members. Such attacks can compromise

the integrity of family accounts, leading to financial loss, identity theft, and privacy breaches.

Second, our findings refute the null hypothesis, revealing a significant impact of cybercrime on STEM students' interest towards their academic pursuits (χ^2 = 47.499, $p<0.05$). This result supports of Bidgoli et al. (2018). While corroborating the above findings, Broadhurst et al. (2018) highlighted the role of cybersecurity incidents in shaping individuals' perceptions and behaviors, including their interest and involvement in academic endeavors. In essence, when STEM students experience cyber threats targeting their family accounts, they may develop heightened concerns about the security and trustworthiness of online platforms and digital technologies. Consequently, these concerns may impact their motivation and engagement in academic activities (Chang et al., 2023). Therefore, addressing the vulnerabilities inherent in family accounts and promoting a culture of cybersecurity awareness, educators and parents can mitigate the negative impact of cybercrime on STEM students' interest and ensure their continued academic success and digital resilience.

Conclusion

In conclusion, the findings emphasize the vulnerability of family accounts to cybercrime and as well unveils a tangible link between these cybercrime-induced disruptions and shifts in students' interest, and pursuit of STEM education. These findings underscore the importance of implementing robust cybersecurity measures and educational initiatives to mitigate cyber threats and support STEM students' academic success and well-being. Ultimately, this study contributes to research by educating STEM researchers, higher institutions of learning, parents and students on the impact of cyberthreats on STEM students learning. We therefore recommend that the IT industries provide applications that enables heightened and proactive measures to safeguard family accounts towards nurturing sustained interest and progress in STEM education. In addition, students and family members should also acquaint themselves with basic security knowledge to mitigate future occurrences that may affect family relationships.

References

Adaramola, Z (2024). *Daily Trust*, 6 February. FG Probes GTB, Zenith Bank over Data Breach https://dailytrust.com/fg-investigates-two-banks-over-data-breach/

Adenusi, D. A., Adekunle, A. U., Ekuewa, J. B., & Ayediran, O. R. (2020). Challenges and way out of cyber security issues in Nigeria. *Villanova Journal of Science, Technology and Management*, *2*(1).

Al-Hakimi, A., & Nur, M. (2023). Cybercrime Threats in Technology Era. *Journal of Computer Science & Computational Mathematics*, *13*(1), 21-30.

Ayub, O, & Akor, L. (2022). Trends, patterns and consequences of cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences* 5, No. 1: 241-262.

Baller, S., Dutta, S., & Lanvin, B. (2016). *Global information technology report 2016*. Geneva: Ouranos.

Berozashvili, (2024) T. Securing Digital Identities In the Era of remote identity verification. DOI: 10.13140/RG.2.2.11839.11688

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. *Available at SSRN 3176319*.

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., Wang, V. (2021). Victims of Cybercrime: Understanding the Impact Through Accounts. In: Weulen Kranenbarg, M., Leukfeldt, R. (eds) Cybercrime in Context. Crime and Justice in Digital Society, vol I. Springer, Cham. https://doi.org/10.1007/978-3-030-60527-8_9

Bidgoli, M; Knijnenburg, B.P & Grossklags, J. "When cybercrimes strike undergraduates," *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, Canada, 2016, pp. 1-10, doi: 10.1109/ECRIME.2016.7487948.

Clemons, E. K., Dewan, R. M., Kauffman, R. J., & Weber, T. A. (2017). Understanding the information-based transformation of strategy and society. *Journal of Management Information Systems*, *34*(2), 425-456.

Cohen L. E., & Felson M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588–608.

DeLiema, M (2017). Elder Fraud and Financial Exploitation: Application of Routine Activity Theory, *The Gerontologist*, Volume 58, Issue 4, August 2018, Pages 706–718, https://doi.org/10.1093/geront/gnw258

Edidiong, A; Adebanji, A; Bolaji; O, O; Oluwaseun, E.O; & Shola, J.O (2023). Integrating The Implication of Cybercrime Occurrences in Nigeria on Nigerian Students' External Image: A Study on Selected States in the United States of America. *Journal for Reattach Therapy and Developmental Diversities*, *6*(7s), 1113–1130. https://doi.org/10.53555/jrtdd.v6i7s.2806

Fang, M., Jandigulov, A., Snezhko, Z., Volkov, L., & Dudnik, O. (2021). New technologies in educational solutions in the field of STEM: The use of online communication services to manage teamwork in project-based learning activities. *International Journal of Emerging Technologies in Learning (iJET)*, *16*(24), 4-22.

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157-2177.

Kakineen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129-137.

Matazu, S. S. A. (2021). Undergraduates' perception of (STEM) education as a tool for enhancing economic development in Sokoto State, Nigeria. *International Journal of Scientific Research in Science, Engineering and Technology*, *8*(4), 162-170.

Nurse, J. R., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. *arXiv preprint arXiv:1901.01914*.

Pawlicka, A., Choraś, M., & Pawlicki, M. (2020, August). Cyberspace threats: not only hackers and criminals. Raising the awareness of selected unusual cyberspace actors-cybersecurity researchers' perspective. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-11).

Piasecki, S., Urquhart, L., & McAuley, D. (2021). Defense against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Computer Law & Security Review*, *42*, 105542.

Rao, P, S; and Krishna, T. G; & Muramalla, V. S. (2023) Next-gen Cybersecurity for Securing Towards Navigating the Future Guardians of the Digital Realm. *International Journal of Progressive Research in Engineering Management and Science (IJPREMS)*, 3 (9).

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. Anderson Publishing.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, *33*, 2020-01.

Ukam, P. I., Onuh, P. A., Nnaji, D. I., Egbo, E. I., & Ugwu, C. O. (2024). How engagement in internet fraud impact academic activities of undergraduate students in Nigeria: A socio-legal study. *Cogent Social Sciences*, 10(1). https://doi.org/10.1080/23311886.2023.2280285

Chang, V; Golightly, L; Ariel Xu, Q; Boonmee, T; & Liu, B.S (2023) Cybersecurity for children: an investigation into the application of social media. *Enterprise Information Systems*, 17(11), DOI: 10.1080/17517575.2023.2188122