

CYBERSECURITY AWARENESS AND DATA PRIVACY PRACTICES OF LIBRARY AND INFORMATION SCIENCE STUDENTS IN OYO STATE

Omobolanle Seri Fasola, PhD

Department of Library and Information Science,
Emmanuel Alayande University of Education, Oyo

and

Fisayo Oyeyemi Adeniji

University Library,
Emmanuel Alayande University of Education, Oyo

Abstract

This study investigated the influence of cybersecurity awareness on the data privacy practices of undergraduate Library and Information Science (LIS) students in selected universities in Oyo State, Nigeria. The study adopted a quantitative descriptive survey research design. The population comprised 639 undergraduate LIS students from three selected universities in Oyo State, namely Emmanuel Alayande University of Education, Lead City University, Ibadan, and Ladoke Akintola University of Technology, Ogbomoso. Using the Taro Yamane sampling technique, a sample size of 246 respondents was selected. Data were collected through a self-designed questionnaire, while descriptive and inferential statistics were used for data analysis. The findings revealed that the respondents possessed a high level of cybersecurity awareness, with a grand mean of 3.26 for knowledge of cybersecurity concepts and 3.02 for awareness of safe online practices. However, students demonstrated only moderate levels of routine and reflective data privacy practices, with grand means of 2.33 and 2.47 respectively. The study further found that lack of formal cybersecurity training, inadequate privacy education, difficulty in managing privacy settings, and poor privacy habits constituted major challenges to effective data privacy practices. The correlation analysis revealed a significant negative relationship between cybersecurity awareness and data privacy practices among the respondents. The study recommends the integration of cybersecurity and data privacy education into the LIS curriculum and the organization

of regular seminars, workshops, and awareness programmes to promote practical privacy behaviours and improve students' digital security practices.

Keywords: Cybersecurity awareness; data privacy practices; undergraduate Students; cybersecurity training; digital privacy behaviour

Introduction

In the contemporary digital landscape, data privacy has become an increasingly important issue due to the volume and sensitivity of personal information shared online. Data privacy refers to the right of individuals to control how their personal information is collected, used, and stored by organisations or platforms (Felix et al, 2025). With the widespread use of personal data generated daily from names and locations to financial details and health records. When such data falls into the wrong hands, it can lead to identity theft, financial fraud, and breaches of confidentiality. Therefore, protecting individuals' digital information has become a critical priority in ensuring personal safety and maintaining trust in the digital environment.

Data privacy practices refer to the behaviours and precautions individual take to protect their personal information from unauthorized access, misuse, or exposure in digital environments (Ifemeje and Okwuosa, 2021). These practices are increasingly important in the face of rising cyber threats and the exponential growth of personal data shared across online platforms. Common privacy-protective behaviour includes using strong and unique passwords, enabling multi-factor authentication, regularly updating software, limiting the amount of personal information shared online and managing privacy settings on digital platforms. Individuals are also encouraged to avoid using unsecured public Wi-Fi networks for sensitive transactions and to be cautious when

clicking on links or downloading files from unfamiliar sources. These practices help reduce vulnerability to threats like identity theft, data breaches and unauthorized surveillance.

Rousi et al (2024) posit that, among undergraduate students, data privacy practices tend to vary significantly depending on factors such as digital literacy, academic exposure, and personal attitudes toward online security. Many students frequently use online platforms such as email, cloud storage services and social media, often without fully understanding the risks involved. As a result, some may fail to use privacy-enhancing tools or neglect crucial steps like updating passwords or adjusting privacy settings on social media accounts. While many students are aware of general online risks, convenience often takes priority over security, leading to habits such as using the same password for multiple accounts or ignoring warnings about insecure websites.

Closely related to data privacy is the broader concept of cybersecurity, which encompasses the technologies, processes, and practices designed to protect networks, devices, programmes and data from attack, damage, or unauthorized access. Cybersecurity is a fundamental pillar of the digital world, particularly as cyberattacks grow more sophisticated and frequent. From ransomware and phishing scams to data breaches and system infiltrations, the range of cyber threats is vast and evolving. Institutions, businesses and individuals alike face the ongoing challenge of keeping digital systems secure while maintaining usability and accessibility. As such,

cybersecurity is not only a technical concern but also a social and behavioural one, involving everyone who interacts with digital systems.

Despite growing access to cybersecurity information and tools, a large proportion of undergraduates continue to exhibit risky privacy behaviours. Study by Nilupú-Moreno et al, (2024) shows that students are more likely to prioritize functionality and ease of access over data protection, especially when deadlines and academic pressures increase. Additionally, many undergraduates assume they are unlikely targets for cyberattacks and therefore underestimate the consequences of poor data privacy practices. This highlights the need for targeted awareness programmes and digital safety education within academic institutions, aimed at bridging the gap between awareness and responsible action. Promoting a culture of proactive digital self-protection is essential in preparing students to navigate the digital world securely.

Cybersecurity awareness is a key component in mitigating threats and encouraging responsible digital behaviour. It involves understanding potential cyber risks, recognizing suspicious activities and knowing how to respond to threats effectively. For individuals, especially students who are among the most active users of digital technology, cybersecurity awareness can play a vital role in reducing vulnerability to cyber threats, educational initiatives, training programmes and campus campaigns (Adeshola & Oluwajana, 2024). These often aims to raise this awareness, but the effectiveness of such efforts varies. This is the gap in literature that this study intends to fill.

Research question

The following research questions guided the conduct of this study;

- i. What is the level of cybersecurity awareness among undergraduate LIS students in Oyo state?
- ii. What are the routine data privacy practices adopted by undergraduate LIS students in Oyo State?
- iii. What are the challenges faced by LIS undergraduate students in implementing proper data privacy practices?
- iv. What is the the relationship between cyber security awareness and data privacy practices of LIS students in Oyo state?

Literature review

Cybersecurity refers to the practices, technologies and processes designed to protect computer systems, networks and digital data from unauthorized access, attack, damage, or theft. It encompasses measures that defend against a wide range of threats, including viruses, malware, phishing, ransomware and hacking (Awodiran et al, 2024). The primary goal of cybersecurity is to ensure the confidentiality, integrity and availability of information often referred to as the CIA triad. These principles guide the protection of both personal and organisational data across digital environments. Sulyman and Makinde, (2024) posits that the field of cybersecurity extends beyond technical tools to include user behaviour, legal frameworks and organisational policies. Effective cybersecurity requires a combination of preventive technologies, such as

firewalls and encryption along with user education and awareness to reduce the risks posed by human error.

The concept is rooted in the broader discipline of information security where the human factor is often considered the weakest link. While technical safeguards such as firewalls and encryption are essential, the effectiveness of these tools is undermined if users lack the awareness to use them correctly. Study by Nurse et al. (2025) highlights that human error is responsible for a large percentage of security breaches, underscoring the importance of educating users to recognize phishing attempts, avoid unsafe downloads and maintain secure passwords. Therefore, awareness is not only about knowledge acquisition but also about developing habits that reduce vulnerability to cyber incidents.

Study by Zwilling et al (2022) on the relationships between cyber security awareness, knowledge and behaviour with protection tools among individuals in general and across four countries; Israel, Slovenia, Poland and Turkey in particular, reveal that internet users possess adequate cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones. The study also show that higher cyber knowledge is connected to the level of cyber awareness, beyond the differences in respondent country or gender.

Bada et al (2019) studied cyber security awareness campaigns in order to identify key factors regarding security which may lead them to failing to appropriately change people's behaviour. The authors' reviewed literature on the suitability of persuasion

techniques, included the widely used 'fear appeals.' From this range of literature, the extracted essential components revealed findings for an awareness campaign as well as factors which can lead to a campaign's success or failure. Finally, they presented examples of existing awareness campaigns in different cultures (the UK and Africa) and reflect on these. Findings from the study revealed a moderate level of awareness of cybersecurity.

Al-Janabi and Al-Shourbaji (2016) researched cybersecurity awareness in educational environment in the Middle East, with the main goal of analysing the information security awareness among academic staff, researchers, undergraduate and employees within educational environments in the Middle East. The results revealed that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. They found that the level of cybersecurity awareness of the respondents was low.

Data privacy practices refer to the actions and behaviours individuals adopt to control the collection, use and sharing of their personal information in digital environments. These practices are essential in safeguarding sensitive data such as login credentials, financial records, personal identifiers and communication history. According to Yan et al (2024), data privacy is rooted in the right to informational self-determination, where individuals decide how their data is handled. Common privacy practices include using strong and unique passwords, enabling two-factor

authentication, adjusting privacy settings on social media platforms, regularly updating software and being cautious about the websites and applications one interacts with.

Scholars have emphasized that effective data privacy practices are not solely dependent on technical knowledge but also on users' attitudes, perceptions of risk and digital habits. Research by Ebenibo et al (2024), found that even when individuals are aware of privacy risks, they often fail to adopt protective behaviours due to convenience, lack of motivation or a belief that their data is not valuable. Therefore, data privacy practices were shown to be low.

The concept of data privacy practices centres on the behaviours and strategies individuals and organisations use to protect personal and sensitive information in digital environments. As digital technologies continue to permeate everyday life, the amount of personal data shared online has increased significantly, raising concerns about how such information is collected, stored and used. According to Yan et al (2024), data privacy involves the right of individuals to control information about themselves and data privacy practices are the means by which this right is exercised in practical terms. These include actions such as managing privacy settings, limiting data disclosure, using secure passwords and being selective about the platforms where personal data is shared.

Study by Sulyman and Makinde (2024) showed the relationship between undergraduate students at Al-Hikmah University in Ilorin, Nigeria and their understanding of cyber-security and data privacy practices. A sample of 200 students

was randomly selected from among the entire population. The findings of the study revealed that students have a moderate grasp of cyber-security procedures, with privacy concerns and proactive adoption of protective measures standing out. The overall average mean score of 3.42, indicated a good level of adherence to essential cybersecurity practices among the surveyed students. Majority of the students responded positively to regularly updating software and security patches on their devices, using strong, unique passwords for online accounts, avoid sharing sensitive information online and doing regular back up of important data. Their responses go to show that the students had good data privacy practices and regularly practiced them.

Methodology

The research design was quantitative using the descriptive survey method. It is particularly effective for studies that seek to determine the relationships among variables. The population for this study were all library and information science students from three selected universities in Oyo state, Ladoke Akintola University, Ogbomosho, Lead City University, Ibadan and Emmanuel Alayande University of Education, Oyo, a total of 639 respondents. The Taro Yamane (1967) sampling technique was used to select 246 with 0.05% margin of error and 5% precision. The instrument for collecting data for the research is a self-designed questionnaire. Data collected was analysed using simple and inferential statistics and the only hypothesis postulated was analysed using PPMC at 0.05 level of significance

Findings and discussion

Table 1. Demographic profile of the respondents

Variable		Frequency	Percent
Gender	Male	114	46.3
	Female	132	53.7
University	Emmanuel Alayande University of Education	82	33.33
	Lead City University, Ibadan	82	33.33
	Ladoke Akintola University of Technology	82	33.33
Level	100 level	75	30.5
	200 level	67	27.2
	300 level	56	22.7
	400 level	48	19.5
Age	16-20 years	152	61.8
	21-25 years	77	31.3
	26-30 years	14	5.7
	31yrs upwards	3	1.2

Table 1 shows the demographic profile of the respondents. Females are in the majority (53.7%) in relation to males (46.3%). All the universities used were equally sampled with mean of (33.33) for each. The distribution across academic levels shows that the majority of respondents are in the lower levels of study. Specifically, 100-level students accounted for 30.5% and 200-level students for 27.2%, together making up 57.7% of the sample. However, 300-level (22.7%) and 400-level students (19.5%) are less represented. The age distribution reveals that most respondents are young, with 61.8% aged between 16–20 years and 31.3% between 21–25 years. Only a very small proportion (1.2%) fall within the 31 years upwards category.

Table 2 below presents respondents' level of formal training in cybersecurity or data privacy.

Table 2: Formal training on cybersecurity or data privacy

Response	Frequency	Percent
----------	-----------	---------

Yes	90	36.6
No	156	63.4
Total	246	100.0

The results show that a majority of respondents (63.4%) indicated that they have **not** received any formal training in cybersecurity or data privacy, while only 36.6% reported that they have undergone such training.

Research Question 1: What is the level of cybersecurity awareness among undergraduate LIS students in Oyo state?

Table 3: Level of Cybersecurity Awareness

	Strongly Disagree	Disagree	Agree	Strongly Agree	Mean
Knowledge of cybersecurity concepts					
I understand what cybersecurity means		3(1.2%)	162(62.3%)	95(36.5%)	3.35
I can identify examples of cyber threats such as phishing or malware		22(8.5%)	142(54.6%)	96(36.9%)	3.28
I know how to adjust privacy settings on social media accounts	5(1.9%)	47(18.1%)	115(44.2%)	93(35.8%)	3.14
I know that clicking unknown links or email attachment can be dangerous		22(8.5%)	105(40.4%)	133(51.2%)	3.43
I am familiar with 2-factor authentication and how it enhances security	8(3.1%)	26(10.0%)	159(61.2%)	67(25.8%)	3.10
Grand mean					3.26
Awareness of safe online practices					
I am aware of the importance of using strong and unique passwords		29(11.2%)	58(22.3%)	173(66.5%)	2.25
I am aware that using unsecured public Wi-Fi can expose me to cyber threats		26(10.0%)	126(48.5%)	108(41.5%)	3.32
I regularly check the authenticity of websites before submitting personal information	3(1.2%)	69(27.5%)	96(38.2%)	83(33.1%)	3.03
I understand the risks of	15(5.8%)	51(19.6%)	66(25.4%)	128(49.2%)	3.18

sharing personal data with
unverified apps or websites

Grand mean 3.02

Exposure to cybersecurity information

I have received formal training or lectures on cybersecurity in my department 49(18.8%) 51(19.6%) 144(55.4%) 16(6.2%) 2.49

I have learned about cybersecurity through media (e.g blogs, news, social media) 6(2.3%) 46(17.7%) 88(33.8%) 120(46.2%) 3.24

My university provides useful information about safe internet use 3(1.2%) 78(30.0%) 104(40.0%) 75(28.8%) 2.97

I have attended workshops or seminars on online safety and data protection 6(2.3%) 45(17.3%) 145(55.8%) 64(24.6%) 3.03

I actually seek information about how to stay safe online 22(8.6%) 64(21.0%) 74(28.8%) 107(41.6%) 3.03

Grand mean 2.95

(0-1.50=low; 1.51-2.49=moderate; 2.50 and above =high)

Table 3 reveals information on level of awareness of cybersecurity. Level of cybersecurity awareness was tested using three dimensions; knowledge of cybersecurity concepts, awareness of safe online practices and exposure to cybersecurity information. Out of these three dimensions, knowledge of cybersecurity concepts was shown to have the highest mean of 3.26, while exposure to cybersecurity information showed the lowest mean (2.92). However, all of the indicators together, returned a mean above 2.50, implying a high level of cybersecurity awareness. This aligns with Bada et al (2019) indicating that while LIS students possess conceptual and practical awareness, this awareness is not uniformly comprehensive, suggesting that awareness programmes may exist but are either inadequate or inconsistently applied.

Research Question 2: What are the common data privacy practices adopted by undergraduate LIS students in Oyo State?

Table 4: Common data privacy practices

	Never	In the past 6 months	In the past 3 months	In the past month	In the past weeks	Mean
Changed the password for your main accounts	108(41.5%)	62(23.8%)	59(22.7%)	19(7.3%)	12(4.6%)	2.10
Changed the password for your social media accounts	109(41.9%)	78(30.0%)	46(17.7%)	10(3.8%)	17(6.5%)	2.03
Logged out of your accounts on a shared or public computer	86(34.4%)	60(24.0%)	56(22.4%)	27(10.8%)	21(8.4%)	2.34
Reviewed and updated privacy settings on your social media account(s)	72(27.7%)	85(32.7%)	57(21.9%)	38(14.6%)	8(3.1%)	2.33
Avoided connecting to public Wi-Fi for private tasks like banking or email	81(31.2%)	65(25.0%)	82(31.5%)	29(11.2%)	3(1.2%)	2.26
Deleted cookies or browser history for privacy reasons	7(2.8%)	112(44.8%)	79(31.6%)	44(17.6%)	8(3.2%)	2.73
Checked app permission on your mobile phone and made changes	80(30.8%)	87(33.5%)	67(25.8%)	23(8.8%)	3(1.2%)	2.16
Updated antivirus or security software on your devices	82(31.5%)	51(19.6%)	47(18.1%)	25(9.6%)	55(21.2%)	2.69
Grand mean						2.33

(0-1.50=low; 1.51-2.49=moderate; 2.50 and above =high)

Tables 4 and 5 are used to answer research question 2. Table 4 reveals the common data practices of the respondents. 'Deleted cookies or browser history for privacy reasons' was the most common data privacy practice adopted by undergraduates while 'changed the password for your social media accounts' was the

least data privacy practice adopted. The entire scale returned a grand mean of 2.33 which implies moderacy.

Table 5: Reflective data privacy behaviour

Statement	I don't do this and don't think it's important	I know it's important but I don't do it	I occasionally do this	I regularly do this	I do this automatically as part of my routine	mean
Use different passwords for different accounts	115(46.9%)	47(19.2%)	64(26.1%)	6(2.3%)	13(5.0%)	1.99
Read the privacy policy or terms and conditions before using a website or app	88(33.8%)	113(43.5%)	34(13.1%)	16(6.2%)	9(3.5%)	2.02
Limits the amount of personal information shared online	65(25.0%)	79(30.4%)	51(19.6%)	52(20.0%)	13(5.0%)	2.50
Avoid clicking on suspicious links or ads on websites and social media	47(18.1%)	119(45.8%)	63(24.2%)	22(8.5%)	9(3.5%)	2.34
Review the permissions app request before installing them	45(17.3%)	88(33.8%)	68(26.2%)	59(22.7%)		3.37
Use 2-factor authentication when its available	66(26.4%)	90(34.6%)	62(23.8%)	16(6.4%)	16(6.4%)	2.32
Think carefully before accepting cookies on websites	40(16.0%)	72(28.8%)	93(37.2%)	27(10.8%)	18(7.2%)	2.64
Discuss or learn about data privacy topics with my peers, lecturers or online sources	40(16.0%)	87(33.5%)	82(31.5%)	28(11.2%)	13(5.2%)	2.55
Grand mean						2.47

(0-1.50=low; 1.51-2.49=moderate; 2.50 and above =high)

Table 5 shows the reflective data privacy behaviour of students. ‘Review the permissions app request before installing them’ returned the highest mean of 3.37 while ‘use different passwords for different online accounts’ returned the lowest mean. The grand mean of 2.47 showed that the respondents exhibited moderate reflective data privacy behaviour.

Taken together, findings from the two scales testing common data privacy practices and reflective data privacy behaviour indicate that students’ engagement with privacy measures is moderate but inconsistent. While basic measures are practiced, more critical actions like regularly changing passwords and using different passwords across accounts are infrequently implemented. Reflective practices such as reading privacy policies and limiting personal data sharing were largely neglected. This suggests that while awareness exists, habitual and proactive adoption of privacy practices is low, confirming Dunmade et al’s (2024) study on university students’ cybersecurity behaviour. The discrepancy between routine actions and reflective behaviours is an indication of the need for practical, behaviour-oriented training that emphasizes not just awareness but habit formation and application.

Research question 3: What are the challenges faced by LIS undergraduate students in implementing proper data privacy practices?

Table 6: Challenges faced in implementing proper data privacy practices

Statements	Strongly disagree	Disagree	Agree	Strongly agree	Mean
I lack knowledge about managing privacy settings effectively	25(10.0%)	31(12.4%)	96(38.4%)	98(39.2%)	3.07
I sometimes forget to log out of shared devices	17(6.8%)	75(30.0%)	83(33.2%)	75(30.0%)	2.86
Managing data privacy is too		78(31.2%)	130(52.0)	42(16.8%)	1.86

time-consuming					
I assume default privacy settings are already safe	14(5.8%)	60(25.0%)	97(40.4%)	69(28.8%)	2.92
Apps and platforms don't clearly explain how to protect data	28(11.2%)	15(6.0%)	126(50.4%)	81(32.4%)	3.04
I have never received formal training on cybersecurity	14(5.6%)	34(13.6%)	112(44.8%)	90(34.6%)	3.08
My university does not provide enough education on digital privacy	52(20.8%)	67(26.8%)	75(30.0%)	56(21.5%)	2.52
Me devices do not support advanced privacy features	15(6.0%)	32(12.8%)	152(60.8%)	51(20.4%)	2.96
I often have to use insecure public Wi-Fi	34(13.6%)	41(16.4%)	89(35.6%)	86(33.1%)	2.88
My peers don't take data privacy seriously	24(9.6%)	62(24.8%)	89(35.6%)	75(30.0%)	2.86
I feel social pressure to share personal information online		40(16.7%)	97(40.4%)	103(39.6%)	2.23
I trust popular platforms and don't worry much about risks		40(16.0%)	160(64.0%)	50(19.2%)	2.03
Privacy concerns seem exaggerated	10(3.8%)	92(36.8%)	86(34.4%)	62(34.8%)	3.33
I believe nothing can fully protect my data once it is online		27(10.8%)	105(42.0%)	118(47.2%)	2.36
I find it difficult to remember multiple passwords	29(11.6%)	42(16.8%)	121(48.4%)	58(23.2%)	2.83
Grand mean					2.79

(0-1.50=low; 1.51-2.49=moderate; 2.50 and above =high)

Table 6 revealed the challenges the students faced in the implementation of proper data privacy practices. The major challenge identified by the students is 'privacy concerns seem exaggerated' with mean of (3.33) while the least challenge faced was 'never having received formal training on cybersecurity' with mean (1.86). However, all of the statements showed a mixture of low and high mean with a grand mean (2.79). Since this is over the 2.49 threshold for moderate, one can safely say that the challenges faced in proper implementation of data privacy by the respondents was high. This aligns with Klymenko et al (2023), demonstrating that students' ability to implement privacy measures is influenced not only by knowledge but also by external constraints and

psychological factors, highlighting the need for comprehensive strategies that address these multifaceted challenges.

Research Question 4: What is the relationship between cyber security awareness and data privacy practices of LIS students in Oyo state?

Table 7: Correlations between cybersecurity awareness and data privacy practices

		Routine data privacy practices	Reflective data privacy practices
Knowledge of cybersecurity concepts	Pearson	-.131*	-.118
	Correlation		
	Sig. (2-tailed)	.038	.071
	N	250	235
Awareness of safe online practices	Pearson	-.276**	-.521**
	Correlation		
	Sig. (2-tailed)	.000	.000
	N	241	226
Exposure to cybersecurity information	Pearson	-.356**	-.383**
	Correlation		
	Sig. (2-tailed)	.000	.000
	N	247	232

The results show a weak negative correlation between knowledge of cybersecurity concepts and common data privacy practices ($r = -0.131$, $p = 0.038$), which is statistically significant at the 0.05 level. However, the correlation with reflective data privacy practices ($r = -0.118$, $p = 0.071$) is not statistically significant.

Awareness of safe online practices is negatively and significantly correlated with both common ($r = -0.276$, $p < 0.01$) and reflective data privacy practices ($r = -0.521$, $p < 0.01$).

The stronger negative correlation with reflective practices indicates that higher awareness of safe online behaviour is associated with lower engagement in reflective privacy practices. This counterintuitive result may reflect a disconnect between perceived awareness and actual practice, where students might feel confident in their

online safety knowledge but fail to apply it consistently. It may also suggest overconfidence, leading to complacency in adopting deliberate privacy measures. Exposure to cybersecurity information shows a moderate negative correlation with both routine ($r = -0.356$, $p < 0.01$) and reflective data privacy practices ($r = -0.383$, $p < 0.01$). The correlation analysis demonstrates that there is a statistically significant but negative relationship between cybersecurity awareness and data privacy practices among LIS students in Oyo State. This finding contradicts Sulaiman and Makinde (2024) on cybersecurity awareness and data privacy practices.

Recommendations

1. Cybersecurity and data privacy education should be inculcated into the LIS curriculum. Since a majority of the students had not received formal training in cybersecurity, management of universities should introduce dedicated courses or modules on cybersecurity awareness and data privacy to equip students with practical digital security skills.
 2. Regular seminars, workshops, and awareness campaigns should be organized for students. The findings revealed limited exposure to formal cybersecurity training and workshops. Therefore, universities should frequently organize training programmes and awareness campaigns on emerging cyber threats and safe online practices.
 3. Students should be encouraged to adopt practical privacy protection habits.
- Although the respondents demonstrated relatively high awareness of

cybersecurity concepts, their actual privacy practices were only moderate. Students should therefore be encouraged to regularly change passwords, use different passwords for different accounts, and enable two-factor authentication.

4. Behavioural-based cybersecurity training should be emphasized. Awareness alone was found not to translate into effective privacy practices. Training programmes should therefore focus on developing positive digital habits and practical skills rather than merely providing theoretical knowledge.
5. Peer learning and discussion on data privacy should be encouraged among students. Departments and student associations should create opportunities for discussions, peer education, and digital safety clubs that promote responsible online behaviour and information sharing practices.

Conclusion

This study examined the influence of cybersecurity awareness on the data privacy practices of undergraduate library and information science students in selected universities in Oyo State. The findings revealed that the students possess a relatively high level of cybersecurity awareness, particularly in their knowledge of cybersecurity concepts and safe online practices. However, despite this awareness, their actual data privacy practices were only moderate, indicating a gap between knowledge and practical application. Furthermore, several challenges, including lack of formal training, inadequate digital privacy education, difficulty in managing privacy settings, and poor

privacy habits, hindered the effective implementation of data privacy practices among the students. The study also established a significant negative relationship between cybersecurity awareness and data privacy practices, suggesting that awareness alone may not necessarily translate into responsible privacy behaviour.

References

- Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*, 12(4), 1283-1305.
- Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management*, 15(01), 1-30. <http://doi.org/10.1142/S0219649216500076>
- Awodiran, M. A., Ogundele, A. T., Idem, U. J., Ilubusi, B. S., Olutoye, E. A., Jimba, K. I., ... & Ibukun, F. O. (2024; November). *Cyber security awareness and firm-level readiness among small and medium-sized audit firms in Nigeria*. In 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON) (pp. 1-5). IEEE.
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv: 1-11*, 1901.02672.
- Dunmade, A. O., Tella, A., & Onuoha, U. D. (2024). A developed framework for studying cyberethical behaviour in North Central Nigeria. *Journal of Cybersecurity Education, Research and Practice*, 1, article 8. <https://doi.org/10.32727/8.2023.27>
- Ebenibo, L., Enyejo, J. O., Addo, G., & Olola, T. M. (2024). Evaluating the sufficiency of the data protection act 2023 in the age of artificial intelligence (AI): A comparative case study of Nigeria and the USA. *International Journal of Scholarly Research and Reviews*, 5(01), 088-107.
- Felix, A., Abdullahi, A., Momoh, J., Ikpaya, I. D., & Juliet, I. O. (2025, February). *Strengthening data privacy and protection in Nigeria: recommendations for a comprehensive approach*. In 8th URSI-NG Annual Conference (URSI-NG 2024) (pp. 27-38). Atlantis Press.
- Ifemeje, S. C., & Okwuosa, N. M. (2021). Data privacy protection: overview of the legal framework in Nigeria. *IRLaw Journal*, 14 (3), 111-118.
- Klymenko, O., Meisenbacher, S., & Matthes, F. (2023). Identifying practical challenges in the implementation of technical measures for data privacy compliance. *arXiv preprint arXiv:2306.15497*.

- Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe-Soto, M., & Riega-Virú, Y. (2024). *Cybersecurity in university students: a systematic review of the literature*. In International conference on WorldS4 (pp. 315-332). Springer, Singapore.
- Nurse, J. R., Milward, J., & Alashe, O. (2025, June). *From security awareness and training to human risk management in cybersecurity*. In International Conference on Human-Computer Interaction (pp. 86-104). Cham: Springer Nature Switzerland.
- Rousi, R., Alanen, H. K., & Wilson, A. (2024). *Data privacy, ethics and education in the era of AI-A University Student Perspective*. 7th Conference on Technology Ethics (TETHICS2024), November 6-7, 2024, Tampere, Finland
- Sulyman, B. M. & Makinde, O. S. (2024). Cyber-security awareness and practices among undergraduate students: a study on artificial intelligence, privacy concern, and data protection. *International Journal of Innovative Technology Integration in Education*, 7(1), 110-119.
- Yan, B., Li, K., Xu, M., Dong, Y., Zhang, Y., Ren, Z., & Cheng, X. (2024). On protecting the data privacy of large language models (llms): A survey. *arXiv preprint arXiv:2403.05156*.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97.