PUSTAKALAY RESEARCH JOURNAL OF INFORMATION TECHNOLOGY AND LIBRARY SCIENCE
An International Peer-Reviewed Journal of Library & Information Science
ISSN: 3048-4960 | Vol. 3, Issue No. 1, Jan–Jun 2026
BMS PUBLISHING HOUSE, NEW DELHI | www.bmsgroup.in
DOI:10.5281/zenodo.22058497 |PRJITLS.V3P42026

Cybersecurity Awareness Programs in Libraries: An Analysis of the Role of Users' Perception and Impacts on Digital Security

Md Soleman Pharcy
Librarian, Jakir Hossain Medical College and Research Institute
Murshidabad, West Bengal – 742224

Emran Ali
Librarian, Lalgola Madanmohan Roy Teachers Training College
Murshidabad, West Bengal-742224

Abstract

Abstract: Cybersecurity has become a critical issue for libraries today, as they rely more on digital technologies to provide information, communication tools, and library services. Risks like phishing, malware, ransomware, identity theft, and data breaches threaten library users, making it essential to implement awareness programs that enhance users' knowledge and promote safer online behaviors. This study explores how such programs influence users' understanding and attitudes toward digital security. A descriptive survey was conducted involving 100 participants from academic and public libraries. Data were gathered through questionnaires, interviews, and group discussions to evaluate users' views on cybersecurity awareness efforts. The results indicated that half of the participants had a moderate level of awareness, while 35% had a high level. Furthermore, 80% of participants either agreed or strongly agreed that these programs were effective in strengthening their knowledge. The analysis found a statistically significant connection between participation in awareness activities and increased cybersecurity awareness ($\chi^2 = 12.84$, $p = 0.012$). Overall, the findings show that involvement in cybersecurity programs improves user awareness, highlighting the important role of libraries in promoting online safety. The study suggests integrating cybersecurity education into existing information literacy efforts and broader library services. This supports the development of knowledgeable communities and strengthens users' ability to protect themselves from cyber threats.

Keywords: Cybersecurity Literacy, Library Users, Information Security, Cyber Awareness, Digital Literacy, User Perception, Library Services, Cyber Threats, Information Literacy

1. Introduction

Introduction: Cybersecurity safeguards systems, networks, devices, and information against unauthorised access, attacks, and theft. GPT-powered CSAT programmes provide a scalable and cost-effective way to enhance cybersecurity awareness through tailored training materials that equip individuals to respond to cybersecurity threats relevant to their unique roles within the organisation (Nabil Al-Dhamari, Nathan Clarke 2024).As centres for information, libraries manage large amounts of sensitive data, making them attractive targets for cybercriminals. Users engage with digital resources through public computers, local networks, mobile applications, and remote connections—each of

which can introduce security risks. Cybersecurity awareness programs can assist users in better understanding online threats and adopting safer practices. Given their role as community knowledge centres, libraries are well-suited—and arguably responsible—for delivering cybersecurity education. Understanding how users perceive these programs is important in creating effective interventions and enhancing digital protection. Therefore, this study focuses on user perceptions of cybersecurity awareness programs within library environments.

2. Literature Review:

Edmont Pasipamire's (2025) carried out a detailed review of cybersecurity practices in the library and information field, identifying libraries as essential players in providing training, integrating cybersecurity with digital literacy, engaging stakeholders, and conducting ongoing evaluations to create effective awareness programs. In 2024, the National Institute of Standards and Technology (NIST) released Cybersecurity Framework_(CSF)_2.0, expanding its original focus on critical infrastructure to all organizations.

Cosmin Mihai (2024) assessed ENISA's AR-in-a-Box model, which offers guidance for creating impactful awareness campaigns based on stakeholder communication needs, program goals, and regular assessments. The research highlights the value of applying established frameworks when implementing cybersecurity initiatives in libraries.Kate-Riin KONT (2023) examined information security practices in Estonian libraries, identifying factors such as document handling, email usage, social media activity, and incident reporting as influential in shaping staff behavior.

ENISA has actively worked with partners to develop educational materials and raise awareness about cybersecurity. In 2024, it launched the ENISA Cyber Education Platform to support skill development among various groups. Over the years, the agency has promoted cybersecurity education as a way to strengthen digital sovereignty and build a more secure digital environment.

Recent analyses show that cybersecurity education can significantly improve an organization's security maturity and reduce the number of incidents. Consistent user involvement in awareness activities contributes to a stronger cybersecurity culture. Additionally, emerging technologies like generative artificial intelligence are being explored as tools for delivering cybersecurity training to students, staff, and library users—an innovation with potential for wider application in the sector.

The International Federation of Library Associations and Institutions (IFLA, 2024) has emphasized the importance of digital adaptability, information literacy, and knowledge management competencies in the modern information landscape.

Multiple studies reinforce the need to build digital skills—including cybersecurity awareness—among the public, with library users identified as a key group benefiting from such initiatives. Kont (2024) examined information security practices in Estonian libraries, identifying factors such as document handling, email usage, social media activity, and incident reporting as influential in shaping staff behavior.

The study calls for regular cybersecurity training for library staff to improve awareness and organizational preparedness. Similarly, Gujar et al. (2024) suggest that frameworks like the NIST Cybersecurity Framework, ISO/IEC 27001, and Zero Trust Architecture can guide the development of strong cybersecurity policies and awareness programs in academic libraries, supporting both operational integrity and digital safety.

The importance of information literacy is also widely recognized. Ghosh and Barui (2024) found that while many public library users in West Bengal, India, have basic digital skills, they still require formal

training to improve their digital security competencies. This indicates a need for greater investment in educational programs by both academic and public libraries.

Idhalama, Makori, and Oredo (2025) explored how digital knowledge affects university library service quality, finding a strong correlation between users' digital proficiency and their satisfaction with services. The study recommends increased investment in digital knowledge programs to enhance both service delivery and student capabilities. Likewise, Kont (2025) investigated cybersecurity awareness among librarians in Estonia, Latvia, and Lithuania, uncovering notable differences in knowledge and behavior. The study advocates for sustained training and awareness campaigns to improve librarians' cybersecurity competence and their ability to safeguard information.

Collectively, the literature confirms that cybersecurity is now integral to daily life. Libraries have a responsibility to provide cybersecurity education to protect users from digital threats. While progress has been made, gaps remain—particularly in understanding user perceptions and measuring the real-world impact of awareness programs.

3. Research Gap

Despite growing attention to cybersecurity awareness, its influence on user behavior within library settings—especially in developing countries like India—remains poorly understood. Furthermore, there is limited research assessing how cybersecurity education in libraries translates into actual changes in user practices.

4. Study Objectives:

1. Assess the current level of cybersecurity awareness among library users.
2. Evaluate the impact of cybersecurity awareness programs on users' knowledge and attitudes.
3. Examine the connection between awareness levels and user behavior.
4. Identify the factors affecting users' cybersecurity awareness.
5. Explore the challenges users face in adopting secure online practices.
6. Propose strategies to strengthen cybersecurity awareness in library settings.

5. Research Methodology

A descriptive survey design was used to explore how library users perceive the role of cybersecurity awareness programs in enhancing their knowledge. The study focused on individuals who access library resources digitally. Given the dispersed nature of the population, stratified random sampling was used to select 100 participants from various libraries. Both pri mary and secondary data sources were utilized. Primary data was gathered through surveys, interviews, and focus group discussions, while secondary data came from published and unpublished materials such as journal articles, books, conference papers, and theses. Data analysis involved descriptive and inferential statistics, supported by SPSS software.

6. Hypothesis Testing

To determine whether participation in cybersecurity awareness programs influences users' awareness levels, a chi-square test of independence was conducted.

Null Hypothesis (H_0):

Participation in cybersecurity awareness programs does not predict the level of cybersecurity awareness among library users.

Alternative Hypothesis (H_1):

Participation in cybersecurity awareness programs is associated with higher levels of cybersecurity awareness among library users.

7. Data Interpretation

Table 1: Distribution of Demographic Profiles by Gender and Age

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	55	55%
	Female	45	45%
Age Group	Below 20 Years	30	30%
	21-30 Years	45	45%
	31-40 Years	25	25%

Interpretation: The data show that male respondents made up the majority at 55%, compared to 45% female, indicating a balanced but slightly male-dominated sample drawn from both academic and public library users. In terms of age, the largest group (45%) fell within the 21–30 range, followed by 30% under 20 and 25% between 31 and 40. This age distribution highlights a predominantly young user base, which aligns with higher engagement in digital platforms. Given their frequent use of technology, younger users typically have greater access to online databases, e-journals, and educational content. While this makes cybersecurity awareness especially important for them, it remains equally critical for older users who also rely on electronic resources available through libraries.

Table 2. Distribution of respondents by library type

Library Type	Number of Respondents	Percentage (%)
Academic Library	60	60%
Public Library	40	40%
Total	100	100%

Interpretation: A majority of respondents (60%) were users of academic libraries, while 40% used public libraries. Academic library users typically engage with digital tools such as online journals, databases, and e-books, reflecting the needs of students and researchers. Public library users, on the other hand, offer insight into broader community-level awareness. The higher proportion of academic library users is expected due to the digital demands of academic work. However, including both groups allows for a more comprehensive understanding of cybersecurity awareness across different segments of library users.

Table 3: Level of Cybersecurity Awareness Among Library Users

Awareness Level	Frequency	Percentage (%)
High	35	35%
Moderate	50	50%
Low	15	15%
Total	100	100%

Interpretation: Half of the respondents reported having a moderate level of cybersecurity awareness, while 35% indicated high awareness and 15% low awareness. This suggests that most users possess basic knowledge about cyber threats and protective measures. However, the notable portion with limited awareness remains vulnerable to cyber risks. While foundational understanding is present, there is a clear need to enhance awareness, particularly regarding emerging and complex cyber threats.

Table 4: Participation in Cybersecurity Awareness Programs

Participation Status	Frequency	Percentage (%)
Regularly Participate	30	30%
Occasionally Participate	45	45%
Never Participate	25	25%
Total	100	100%

Interpretation: Nearly half of the respondents (45%) take part in cybersecurity awareness activities occasionally, 30% participate regularly, and 25% do not engage at all. The relatively high number of occasional participants compared to regular ones indicates room for improvement in encouraging consistent involvement. Efforts should focus on making these programs more accessible and engaging, especially for non-participants. Additionally, supporting regular attendees can help ensure they stay informed about evolving threats.

Table 5. User perceptions of cybersecurity awareness programs

Perception	Frequency	Percentage (%)
Highly Effective	35	35%
Effective	45	45%
Neutral	15	15%
Ineffective	5	5%
Total	100	100%

Interpretation: A strong majority (80%) viewed cybersecurity awareness programs positively, with 35% rating them as highly effective and 45% as effective. Only a small fraction expressed neutral or negative views. This favorable perception suggests that users see value in these initiatives and believe they contribute meaningfully to their understanding of cyber risks and protective behaviors.

Table 6. Cybersecurity threats recognized by library users

Cyber Threat	Frequency	Percentage (%)
Phishing Emails	72	72%
Password Theft	68	68%
Malware/Viruses	62	62%
Identity Theft	58	58%
Ransomware	45	45%
Data Breaches	55	55%

Interpretation: Phishing emails were the most widely recognized threat, identified by 72% of respondents, followed by password theft (68%) and malware (62%). Identity theft and data breaches were also commonly acknowledged. In contrast, ransomware was the least recognized, with only 45% identifying it as a threat. This pattern shows that users are more familiar with traditional cyber risks

but less aware of newer or more sophisticated attacks. There is a need to expand education efforts to include less familiar threats like ransomware.

Table 7. Challenges related to cybersecurity faced by library users

Challenge	Frequency	Percentage (%)
Lack of Technical Knowledge	60	60%
Complex Security Procedures	50	50%
Limited Training Opportunities	48	48%
Time Constraints	45	45%
Lack of Awareness Materials	40	40%

Interpretation: The most frequently cited challenge was insufficient technical knowledge, reported by 60% of respondents. Other significant barriers included complicated security processes (50%), limited access to training (48%), time limitations (45%), and lack of educational materials (40%). These findings highlight the importance of simplifying cybersecurity guidance and expanding training access. Providing clear, user-friendly resources could help bridge existing knowledge gaps.

Statistical Analysis (Chi-Square Test)

Table 8. Association between program participation and cybersecurity awareness level

Variable	Chi-Square Value	df	p-value
Participation vs Awareness Level	12.84	4	0.012

Interpretation: The chi-square test yielded a p-value of 0.012, which is below the 0.05 threshold for statistical significance. This means the null hypothesis is rejected, confirming a significant relationship between participation in cybersecurity programs and awareness levels. Users who engage in these programs tend to have higher awareness than those who do not. The results support the effectiveness of such initiatives and underscore the importance of continued investment in awareness campaigns.

Overall Interpretation: The study sheds light on current cybersecurity awareness levels among library users. Most exhibit moderate awareness and benefit from structured programs. Common threats like phishing and malware are well recognized, but knowledge gaps remain—especially regarding ransomware and technical aspects of security. The data confirm a strong link between program participation and improved awareness. To strengthen digital safety, libraries should continue offering and expanding cybersecurity education tailored to diverse user needs.

8. Discussion

The results indicate that while many library users have a basic understanding of cybersecurity, their knowledge is uneven. They are generally aware of common threats such as phishing, password theft, and malware, but less so about advanced risks like ransomware. Participation in awareness programs is mostly occasional, yet users perceive these programs as valuable. Workshops, practical demonstrations, and real-life case studies appear to be particularly effective teaching methods. Overall, attitudes toward cybersecurity education are positive, suggesting that such initiatives are well-received when properly delivered.

Digital literacy emerged as a key factor influencing cybersecurity awareness. Integrating cybersecurity education into existing digital literacy programs could enhance user preparedness. Providing accessible

training materials and ensuring broad availability of cybersecurity instruction are essential steps. Furthermore, the analysis confirms that participation in awareness activities significantly boosts users' knowledge levels. Differences in awareness were also linked to varying degrees of digital skills and technical background, suggesting that programs should be adapted to different user competencies.

Libraries are seen as trustworthy institutions capable of leading cybersecurity education efforts for both academic and general populations. Given their role in promoting information access and digital inclusion, they are well-positioned to foster safer online practices. Expanding their involvement in cybersecurity outreach can help protect users across all experience levels.

9. Findings

i. Most respondents demonstrated a moderate level of cybersecurity awareness.
ii. Users gain measurable benefits from participating in cybersecurity awareness programs.
iii. Phishing, password theft, and malware were the most commonly recognized cyber threats.
iv. Awareness programs are viewed as effective in improving user knowledge.
v. Lack of technical knowledge and limited training access were the primary challenges reported.
vi. A statistically significant link exists between program participation and awareness levels.
vii. Libraries are regarded as credible platforms for advancing cybersecurity education.
viii. Participants in cybersecurity programs showed greater ability to identify potential threats.

10. Recommendations

Based on the findings, the following actions are recommended:

1. Organize regular cybersecurity workshops and seminars.
2. Integrate cybersecurity topics into information literacy curricula.
3. Produce awareness materials in multiple languages.
4. Implement simulated phishing exercises to build vigilance
5. Promote best practices for password creation and management.
6. Encourage adoption of multifactor authentication.
7. Offer online tutorials and live webinars on cybersecurity topics.
8. Partner with IT professionals and cybersecurity experts.
9. Conduct periodic surveys to assess awareness levels.
10. Set up dedicated cybersecurity help desks in academic libraries.
11. Include cybersecurity guidance during new user orientations.
12. Allocate budgetary support for sustained awareness initiatives.

11. Limitations of the study

This study had several constraints. The sample size was limited to 100 participants, which may affect the generalizability of the results. Data collection was confined to few libraries, potentially limiting geographic and institutional diversity. Additionally, the reliance on self-reported survey responses introduces the possibility of response bias. Future research should employ mixed-method designs, incorporate larger and more diverse samples, and include observational or interview-based components to strengthen validity and reduce bias.

12. Conclusion

As digital resource usage grows, so does the need for cybersecurity awareness among library users. The study confirms that awareness programs positively impact users of both academic and public libraries by enhancing their knowledge and promoting safer online behaviors. Libraries play a vital

role in advancing digital literacy and are trusted venues for disseminating cybersecurity education. To further improve user safety, ongoing efforts should focus on expanding access to training, tailoring content to different skill levels, and integrating cybersecurity into routine library services. Special attention should be given to users with lower digital proficiency, ensuring all individuals can navigate online environments securely.

References

1. Al-Dhamari, N., & Clarke, N. (2024). GPT-enabled cybersecurity training: A tailored approach for effective awareness. arXiv. https://arxiv.org/abs/2405.04138

2. European Union Agency for Cybersecurity (ENISA). (2024). Cyber education platform and cybersecurity awareness initiatives.

3. Ghosh, P., & Barui, T. (2024). Assessment of digital literacy skills of the users of public libraries in Kalimpong District of West Bengal, India. College Libraries, 39(4), 41–52.

4. Gujar, S. S., Thiyagarajan, V. S., Sakpal, S. S., & Pandey, A. K. (2024). Advanced cybersecurity frameworks for protecting sensitive information in academic libraries: Innovations and best practices. Library Progress International, 44(3). https://doi.org/10.48165/bapas.2024.44.2.1

5. Idhalama, O. U., Makori, E. O., & Oredo, J. O. (2025). Analyzing the impact of digital literacy practices on the quality of library services and user satisfaction in public university libraries in Nigeria. Information Development. https://doi.org/10.1177/09557490251335951

6. International Federation of Library Associations and Institutions. (2025). IFLA trend report 2024. https://www.ifla.org/trend-report/

7. Rahaman, J., & Batcha, M. S. (2022). A scientometrics assessment of the research performance of Indian universities Shodh Samhita, 9(1), 192–205.

8. Rahaman, J., & Batcha, M. S. (2022). Scientometrics analysis and collaboration trends of state universities from West Bengal. Journal of Social Sciences and Management, 1(2), 21–33.

9. Rahaman, J., & Batcha, M. S. (2022). Scientometrics assessment of the research productivity of Calcutta University, West Bengal. Indian Journal of Natural Sciences, 13(73), 44881–44893.

10. Kont, K.-R. (2023). The role of libraries in creating a safer cyberspace: Awareness of Estonian library employees in information security. The International Information & Library Review, 56(2), 135–149. https://doi.org/10.1080/10572317.2023.2315630.

11. Kont, K.-R. (2025). Measuring information security awareness of librarians: A case study in Estonia, Latvia, and Lithuania. Slavic & East European Information Resources, 26(1–2), 24–49. https://doi.org/10.1080/15228886.2025.2541178

12. Mihai, I.-C. (2024). AR-in-a-Box: A structured 8-step framework for cybersecurity awareness. In International Conference on Cybersecurity and Cybercrime Proceedings (Vol. 11). https://doi.org/10.19107/CYBERCON.2024.05

13. National Institute of Standards and Technology. (2024). Building a cybersecurity and privacy learning program (NIST Special Publication 800-50 Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50r1

14. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The human aspects of the information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

15. Pasipamire, E. (2025). Building a culture of cybersecurity awareness in libraries: A systematic review of best practices and frameworks. In European Conference on Cyber Warfare and Security Proceedings, 24(1). https://doi.org/10.34190/eccws.25.1.3608

16. Suherman, U. (2024). Evaluation of cybersecurity awareness policies using the NIST CSF framework. Quanta Research Journal, 3(2), 45–58.

17. Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004