Library Waves: A Biannual Peer Reviewed Journal of Library and Information Science
Volume 11, Issue 1 (January-June, 2025); ISSN: 2455-2291 (Online); Website: www.librarywaves.com

Digital Engagement and Cyber Literacy among University Students in Southern Rajasthan

*** Jitendra Suhalka#** **** P. S. Rajput**

***** Research Scholar, Department of Library and Information Science, Mohanlal Sukhadia University, Udaipur (Rajasthan) - 313001, INDIA; Email: drjitendrasuhalka@gmail.com
****** Assistant Professor, Department of Library and Information Science, Mohanlal Sukhadia University, Udaipur (Rajasthan) - 313001, INDIA; Email: drpsrajput@mlsu.ac.in
#Corresponding author.

Received: 12 June 2025 ***Accepted: 30 June 2025***

Abstract

This study investigates the patterns of digital engagement and the level of cyber literacy among university students in Southern Rajasthan, focusing on two public institutions: Mohanlal Sukhadia University (MLSU) and Maharana Pratap University of Agriculture and Technology (MPUAT). Using a stratified random sampling method, 150 students were surveyed through a structured questionnaire. The findings reveal high levels of daily social networking site (SNS) usage, primarily for communication, entertainment, and academic purposes. However, awareness of essential cyber safety practices-such as privacy management, password security, and cybercrime reporting was found to be limited. Notably, 18% of respondents reported no familiarity with basic cyber concepts, and 59.33% were unaware of official reporting mechanisms for cyber incidents. Despite these gaps, 84% of students expressed strong support for integrating cyber safety education into university curricula. The study underscores the urgent need for structured digital literacy programs, especially in underrepresented regions. These findings have broader implications for national initiatives like the Digital India Mission and the National Cyber Security Policy, which emphasize digital inclusion, education, and resilience. Enhancing students' cyber competence is vital not only for academic development but also for fostering responsible digital citizenship in India's evolving digital landscape.

Keywords: Digital engagement; cyber literacy; university students; social networking sites; cyber safety; Digital India; Southern Rajasthan.

1. Introduction

The 21st century has witnessed a technological transformation that has fundamentally altered how students interact, communicate, and learn. With the proliferation of digital tools and platforms, social networking sites (SNSs) have become deeply embedded in the academic and social lives of university students. These platforms not only facilitate interpersonal communication but also offer opportunities for collaborative learning, information exchange, personal expression, and digital presence (Pempek, Yermolayeva, & Calvert, 2009). However, while digital engagement is increasingly seen as a necessary skill in the modern academic environment, it also brings challenges related to distraction, misinformation, and cyber threats. In regions such as Southern Rajasthan, where educational aspirations are rising amidst socio-economic and geographic challenges, digital engagement has emerged as both an opportunity

and a concern. University students particularly those from rural and tribal backgrounds, often face barriers related to digital infrastructure, digital literacy and cyber safety awareness.

While students actively use SNSs for various purposes including academic discussions, entertainment, activism, and personal branding. There is often limited understanding of how to navigate these platforms safely and ethically. Cyber literacy, encompassing knowledge of safe digital practices, responsible online behavior, and awareness of cybercrime reporting mechanisms, remains underdeveloped in many higher education settings.

The present study focuses on two interconnected aspects of digital behavior: the level of digital engagement through social networking platforms and the extent of cyber literacy among university students in Southern Rajasthan. By exploring these themes in a socio-culturally diverse region, this research seeks to understand usage patterns, associated risks, and the need for institutional support in promoting safe and productive digital participation.

2. Review of Literature

The widespread integration of digital technologies into higher education has redefined students' academic, social, and personal experiences. An expanding body of research emphasizes that digital literacy is no longer optional but essential for academic success and responsible digital citizenship in the 21st century. Boro, Laltlanzova, and Chanchinmawia (2024) observed that while many Generation Z students at Mizoram University utilize social networking sites (SNSs) for academic purposes, they often lack awareness of cybersecurity and safe digital sharing practices. This highlights a recurring issue: digital engagement and cyber competence must evolve concurrently.

However, earlier studies tend to overlook regional disparities within India. While students may be proficient in using digital platforms for communication and entertainment, they frequently lack the ability to critically evaluate online content. Bansal and Misra (2021) found that although school and university students in India demonstrate functional digital skills, many struggle to assess the credibility of digital information. Likewise, Yadav, Sarin, and Leeladharan (2023) reported that students at Pondicherry University relied heavily on digital tools but showed limited awareness of content validation and ethical digital behavior.

In contrast to these broader national-level studies, the present research focuses on students from public universities in Southern Rajasthan—a region characterized by limited digital infrastructure and underrepresentation in national surveys on digital literacy. This localized emphasis contributes additional contextual depth to the wider discourse on digital engagement in India.

SNSs have become integral to students' academic and personal routines. Boyd and Ellison (2007) define SNSs as platforms that allow users to create profiles, articulate social connections, and participate in digital communities. Although originally developed for recreational use, SNSs now support academic collaboration and expression. In a study conducted at Acharya Nagarjuna University, Babu (2014) reported that over 61% of students believed social media enhanced their academic knowledge, and 62% actively used it to support their studies.

Nevertheless, researchers have also noted the ambivalent effects of SNS usage. Junco (2012) identified a positive relationship between academic use of SNSs and student engagement but also found that excessive non-academic use impaired time management and concentration.

Similarly, Kirschner and Karpinski (2010) reported that frequent Facebook users had lower GPAs than their peers, attributing this to distractions and multitasking.

Digital engagement also shapes students' awareness of cybersecurity. Kant (2023) assessed cybersecurity awareness among Indian university students and noted that although most were active online users, many lacked knowledge of cyber threats and formal reporting mechanisms. These findings underscore the importance of incorporating cyber literacy into broader digital literacy frameworks—particularly knowledge of data protection, privacy, and access to tools such as the Indian Cybercrime Reporting Portal.

Furthermore, digital access alone does not guarantee meaningful participation. Livingstone and Helsper (2007) argue that digital inequality results not only from access disparities but also from differences in the depth and quality of usage. This observation is especially relevant in underrepresented regions such as those studied here, where students may lack institutional support to develop advanced digital competencies.

In summary, while previous research highlights the general need to enhance digital and cyber literacy, the present study contributes by contextualizing these challenges within public universities in Southern Rajasthan. It expands existing scholarship by addressing regional disparities, emphasizing cyber safety behaviors, and evaluating the academic impact of SNS use beyond metropolitan contexts.

Note: To ensure scholarly integrity, this review includes only peer-reviewed studies published up to March 2025. All "in press" or forward-dated sources were excluded to preserve reliability and reproducibility.

3. Objectives of the Study

The study was guided by the following objectives:

1) To explore the extent of digital engagement through social networking sites among university students.
2) To investigate the key purposes for which students utilize social networking platforms.
3) To assess the level of cyber literacy among university students in Southern Rajasthan.
4) To evaluate students' awareness of cybercrime reporting procedures and related mechanisms.
5) To recommend strategies for fostering responsible and informed digital behavior among university students.

4. Scope and Methodology

4.1 Scope of the Study

This study was geographically centred in Southern Rajasthan, focusing on students enrolled at two major public universities in Udaipur: Mohanlal Sukhadia University (MLSU) and Maharana Pratap University of Agriculture and Technology (MPUAT). The research explored students' digital behavior, including their use of social networking sites (SNSs), their awareness of basic cyber safety practices, their knowledge of cybercrime reporting mechanisms, and their attitudes toward incorporating cyber safety education into the university curriculum.

To ensure comprehensive representation, students from diverse faculties and academic levels were included in the sample. However, the study excluded students from private institutions, university faculty and staff (both teaching and non-teaching), and individuals outside the public university system. Therefore, the findings are specific to the public university context in Southern Rajasthan, and their generalizability to other regions or institutional types should be approached with caution.

4.2 Sampling Procedure and Justification

A quantitative survey method was employed for this study. During the 2024-2025 academic session, the student population was approximately 10,500 at MLSU and 3,824 at MPUAT. A stratified random sampling technique was used to ensure proportional representation across faculties and academic years. Based on a 1% sampling strategy, the study targeted 110 students from MLSU and 40 students from MPUAT.

The sampling strategy follows established norms in social science research, especially when applied to finite, well-defined populations. With a 95% confidence level and a ±10% margin of error, the selected sample size strikes a balance between statistical validity and the practical constraints of time and resources (Creswell & Creswell, 2018).

4.3 Data Collection and Management

Structured questionnaires were administered to a slightly larger sample size-140 students at MLSU and 50 at MPUAT to account for incomplete or unreturned responses. Incomplete or missing responses were excluded from the final dataset. Although a non-response bias analysis was not conducted, replacement responses were collected during distribution to preserve proportional representation across strata. Data collection was conducted over a three-week period in March 2025. Students were approached both in person and through official online student groups to maximize participation.

4.4 Instrument Design and Validation

The questionnaire was designed based on a review of relevant literature and feedback from subject-matter experts. Prior to its full-scale deployment, the instrument underwent a pilot test in February 2025 with a sample of 20 students from both universities. Based on the pilot feedback, minor revisions were made to improve question clarity, logical flow, and internal consistency. The pilot confirmed the content validity of the instrument. Reliability was assessed using Cronbach's alpha, which yielded a value of 0.81, indicating strong internal consistency (Taber, 2018).

4.5 Data Processing and Coding

All completed responses were manually reviewed for accuracy and completeness. Responses were numerically coded for statistical analysis using Microsoft Excel. Open-ended responses were cleaned and categorized to ensure consistency in interpretation.

Although personally identifiable information was not solicited in the questionnaire, any inadvertently shared details were anonymized prior to data entry. During processing, all keywords, variable names, and labels were standardized for uniformity. All ethical considerations were strictly observed. This included obtaining informed consent, ensuring voluntary participation, and maintaining the confidentiality of all participant data. Final

conclusions were drawn from the cleaned and validated dataset following structured analysis protocols.

5. Data Analysis and Interpretation

Table - 1: Demographic Characteristics of Respondents (N = 150)

Characteristic	Variables	Frequency (n)	Percentage (%)
Gender	Male	78	52.00
	Female	72	48.00
Residing Area	Rural	62	41.33
	Urban	88	58.67
Age Group	Below 21 years	95	63.33
	21 years and above	55	36.67
Course of Study	Undergraduate (UG)	92	61.3
	Postgraduate (PG)	58	38.67%

Note: Percentages are rounded to two decimal places.

The respondent group includes a total of 150 students. Gender distribution shows a nearly balanced split with 52% male and 48% female students. A majority of respondents (58.67%) come from urban areas, while 41.33% reside in rural regions. Most students are under the age of 21 (63.33%), highlighting the youthful nature of the sample. The academic background is predominantly undergraduate (61.33%), followed by postgraduate students (38.67%).

Table - 2: Daily Duration of Social Networking Site Usage among Students

Time Spent on SNSs (per day)	Number of Respondents (n)	Percentage (%)
Less than 1 hour	22	14.67
1–2 hours	54	36.00
2–3 hours	41	27.33
More than 3 hours	33	22.00
Total	**150**	**100.0**

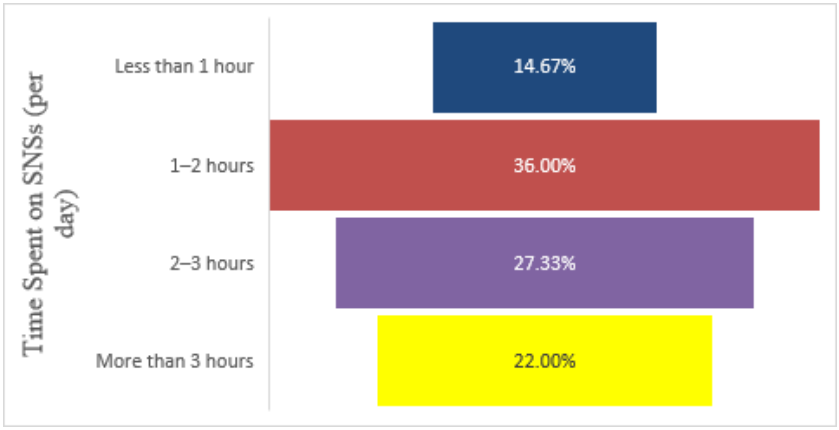

Figure - 1: Daily Duration of Social Networking Site Usage among Students

The majority of students (36%) spend 1-2 hours daily on SNSs. Around 27.33% use SNSs for 2-3 hours, and 22% exceed 3 hours per day. Only 14.67% spend less than an hour on these platforms, indicating that SNSs are a major part of daily routines for most students.

Table - 3: Purposes for Using Social Networking Sites among Students (Multiple Responses Allowed, N = 150)

Purpose of Use	Number of Respondents (n)	Percentage (%)
Communication	120	80.00
Entertainment	115	76.67
Academic Use	106	70.67
News/Updates	89	59.33
Personal Branding	35	23.33
Other (e.g., shopping, hobbies)	15	10.00

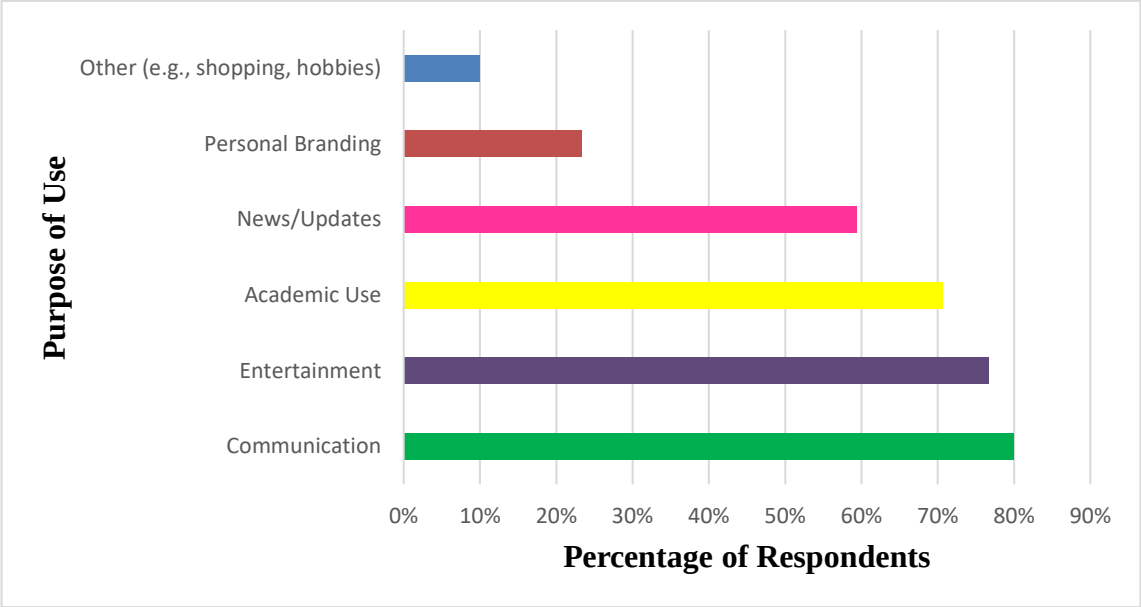

Figure - 2: Purposes for Using Social Networking Sites among Students

Communication (80%), entertainment (76.67%), and academic use (70.67%) are the top reasons for SNS use. News consumption is also popular (59.33%). Fewer students use SNSs for personal branding (23.33%) or other activities (10%).

Table - 4: Awareness of Cyber Concepts among Students (Multiple Responses Allowed, N = 150)

Cyber Concept	Frequency (f)	Percentage (%)
Phishing	73	48.67
Malware/Viruses	83	55.33
Privacy Settings	68	45.33
Strong Password Practices	64	42.67
Cyberbullying	58	38.67
None	27	18.00

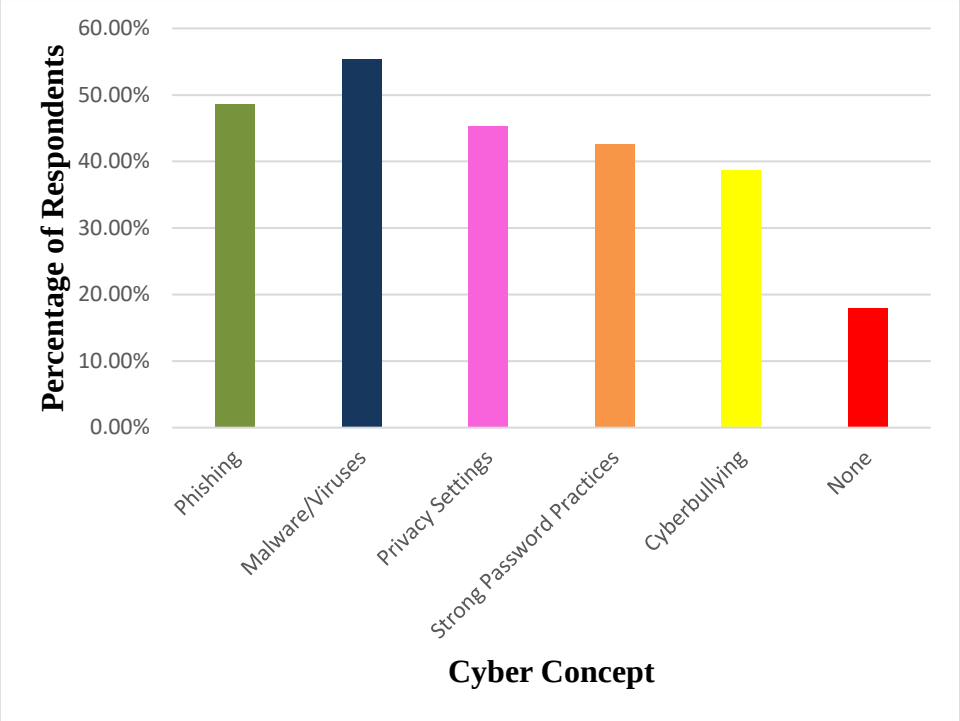

Figure - 3: Awareness of Cyber Concepts among Students

The most recognized concepts are malware/viruses (55.33%) and phishing (48.67%). Awareness of privacy settings and password practices remains below 50%. Cyberbullying awareness is at 38.67%, and 18% of students lack any cyber awareness.

Table - 5: Awareness of Cybercrime Reporting Procedures among Students

Response	Number of Respondents (n)	Percentage (%)
Yes	61	40.67
No	89	59.33
Total	**150**	**100.0**

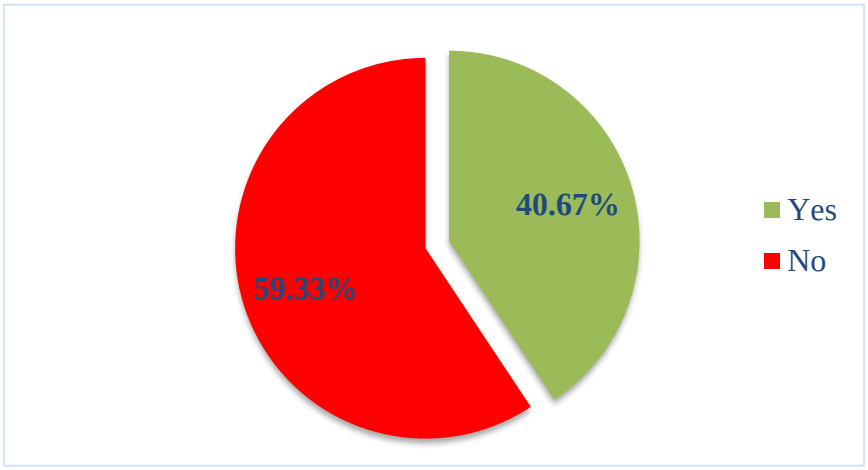

Figure - 4: Awareness of Cybercrime Reporting Procedures among Students

Only 40.67% of students know how to report cybercrime, while the majority (59.33%) are unaware. This indicates a critical lack in practical cyber safety knowledge.

Table - 6: Students' Opinions on Including Cyber Safety in University Curriculum

Response Option	Number of Respondents (n)	Percentage (%)
Strongly Agree	78	52.00
Agree	48	32.00
Neutral	13	8.67
Disagree	7	4.67
Strongly Disagree	4	2.67
Total	**150**	**100**

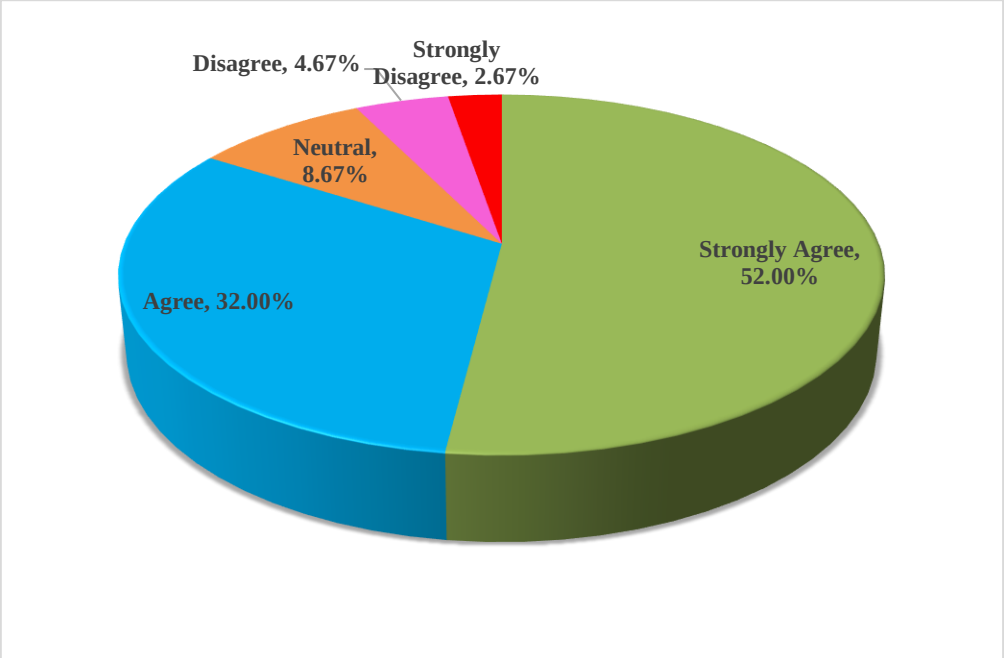

Figure - 5: Students' Opinions on Including Cyber Safety in University Curriculum

A large majority (84%) of students either agree or strongly agree with including cyber safety in the curriculum. Only 7.34% expressed disagreement or indifference, indicating widespread support for formal cyber education.

6. Findings and Suggestions

The study reveals several critical insights into the digital engagement and cyber awareness levels of university students in Southern Rajasthan. The demographic profile indicates that the majority of respondents are undergraduate students under the age of 21, predominantly from urban areas. This demographic is highly active on social networking sites (SNSs), with most students spending over one hour daily on these platforms, and a significant portion exceeding three hours, pointing toward deep digital immersion.

Students primarily use SNSs for communication, entertainment, and academic purposes, showing that these platforms are not only social tools but also support educational activities. However, usage for personal branding and skill development remains low, indicating a lack of awareness about the broader professional and academic potential of these platforms.

In terms of cyber literacy, while more than half of the students are aware of common threats like malware and phishing, knowledge about essential safety practices such as privacy settings,

strong passwords, and cyberbullying is less prevalent. Alarmingly, 18% of students reported no awareness of any cyber concept, highlighting a serious gap in digital safety education. Furthermore, a majority (59.33%) of respondents are unaware of how to report cybercrime, which could leave them vulnerable in the event of a cyber incident.

Despite these gaps, the positive finding is that an overwhelming majority of students (84%) support the inclusion of cyber safety education in the university curriculum. This suggests a strong readiness and demand for structured, formal training in cyber awareness and digital responsibility.

Based on these findings, the following suggestions are proposed

1) **Curriculum Integration**: Universities should incorporate dedicated modules on cyber safety and digital literacy into undergraduate and postgraduate programs, ensuring foundational concepts are taught early.
2) **Digital Wellness Promotion**: Awareness campaigns should be launched to help students manage SNS usage time effectively and balance online engagement with academic responsibilities.
3) **Practical Cyber Education**: Workshops and training sessions should focus on practical topics such as safe browsing, privacy management, phishing detection, cyberbullying prevention, and cybercrime reporting procedures.
4) **Targeted Outreach**: Special attention should be given to undergraduate students, rural students, and those lacking basic awareness, using stratified programs and accessible content formats.
5) **Professional Use of SNSs**: Encourage students to use SNSs for career development, academic networking, and personal branding through platforms like LinkedIn and digital portfolio tools.
6) **Collaboration with Authorities**: Universities can partner with local cybercrime units to provide real-time demonstrations of reporting processes and legal support mechanisms.

By implementing these measures, educational institutions can bridge the gap between digital engagement and cyber awareness, thereby fostering safer, more productive online behavior among students. This alignment is essential not only for academic success but also for responsible digital citizenship in an increasingly connected world.

7. Conclusion

This study explored the patterns of social networking site (SNS) usage and cyber awareness among students of two major state-run universities in Southern Rajasthan: Mohanlal Sukhadia University (MLSU) and Maharana Pratap University of Agriculture and Technology (MPUAT). Findings indicate widespread daily use of SNSs for communication, entertainment, and academic collaboration. While this reflects the increasing centrality of digital platforms in student life, it also raises concerns about distraction, time mismanagement, and insufficient cyber preparedness.

Although the majority of students were familiar with certain cyber threats, their awareness of protective behaviors such as setting strong passwords, using privacy controls, and understanding cybercrime reporting procedures—remained limited. Notably, a significant portion of the sample (18%) lacked knowledge of even the most basic cyber safety concepts. This disconnect between high levels of digital activity and low cyber competence poses risks not only to individual students but also to the broader institutional security framework.

Importantly, student support for cyber safety education was overwhelming. Most respondents favored integrating structured cyber education into academic programs, underscoring a readiness for institutional action.

These findings align closely with national policy goals under the Digital India Mission (MeitY, 2015), which promotes digital empowerment, digital literacy, and inclusive growth. Similarly, the National Cyber Security Policy 2013 (Ministry of Electronics and Information Technology, 2013) advocates cyber awareness and education as key to strengthening national resilience. By investing in digital literacy and cyber hygiene at the university level, institutions can directly contribute to these national objectives.

In conclusion, the study highlights a significant gap between digital consumption and cyber maturity, particularly in semi-urban and underrepresented regions. Bridging this divide is essential not only for academic development but also for building a secure and inclusive digital society. Universities must adopt a proactive role embedding cyber safety in pedagogy, promoting ethical digital behavior, and empowering students to become responsible digital citizens of India's knowledge economy.

References

1. Bansal, C., & Misra, P. K. (2021). Digital literacy of school students in India: A study. *Learning Community: An International Journal of Educational and Social Development, 12*(2), 101-114.https://ndpublisher.in/admin/issues/LCv12n2c.pdf
2. Boro, B., Laltlanzova, R., & Chanchinmawia, F. (2024). Examining digital literacy skills among Gen Z students of Mizoram University. *DESIDOC Journal of Library & Information Technology*, *44*(1), 32-36. https://doi.org/10.14429/djlit.44.1.19291
3. Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230.https://doi.org/10.1111/j.1083-6101.2007.00393.x
4. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
5. Junco, R. (2012). The relationship between frequency of Facebook use, participation in Facebook activities, and student engagement. *Computers & Education, 58*(1), 162-171. https://doi.org/10.1016/j.compedu.2011.08.004
6. Babu, K. J. (2014). *Social media usage among university students: A study in Acharya Nagarjuna University (ANU), India*. Academia.edu. https://www.academia.edu/85608176/Social_Media_Usage_among_University_Students_A_study_in_Acharya_Nagarjuna_University_ANU_India
7. Kant, R. (2023). Cyber-security awareness in India: How much are students of higher education aware? *ResearchGate*. https://www.researchgate.net/publication/371958991
8. Kirschner, P. A., & Karpinski, A. C. (2010). Facebook® and academic performance. *Computers in Human Behavior, 26*(6), 1237-1245. https://doi.org/10.1016/j.chb.2010.03.024
9. Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society, 9*(4), 671-696. https://doi.org/10.1177/1461444807080335
10. Ministry of Electronics and Information Technology (MeitY). (2013). *National Cyber Security Policy 2013*. Government of India. https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf

11. Ministry of Electronics and Information Technology (MeitY). (2015). *Digital India: Power to Empower*. Government of India. https://digitalindia.gov.in
12. Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology, 30*(3), 227-238. https://doi.org/10.1016/j.appdev.2008.12.010
13. Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*(6), 1273-1296. https://doi.org/10.1007/s11165-016-9602-2
14. Yadav, N., Sarin, S., & Leeladharan, M. (2023). Digital literacy and reading habits of the Pondicherry University students. *The Online Journal of Distance Education and e-Learning, 11*(4). https://tojdel.net/journals/tojdel/articles/v11i04/v11i04-07.pdf

■■■