Cybersecurity Awareness and Digital Citizenship among School Students: An Empirical Study of Class XI and XII Students in Bikaner District, Rajasthan

AMARDEEP GODARA

Lecturer in Political Science, Government Senior Secondary School Shivbari , Bikaner , Rajasthan – 334001

ABSTRACT

In recent times, the widespread use of the Internet by various social groups has led to an increase in cyber risks and threats. Consequently, it has become crucial to educate these groups, particularly younger age groups, on the importance of cybersecurity to prevent them from falling victim to these risks. The study will focus on the comprehension of factors affecting cybersecurity among school students and the prevention of cyber threats and risks targeting the younger generation. A cross-sectional survey was conducted on students from middle school in Jordan, using a standardized questionnaire with 37 questions distributed under three categories: demographic data, cybersecurity awareness, and influencing factors. For this particular research study, the responses gathered from the open-ended questionnaire were analyzed, where multiple regression analysis was conducted, and five major research hypotheses were proposed and verified. The results indicate that it can be deduced that the level of knowledge about passwords, social networking sites, and legal aspects influences the level of cybersecurity awareness among the students. Other significant correlates of awareness were self-perceived awareness and education in cybersecurity; the model accounted for 67.5% of the variance in levels of awareness. The study also establishes that awareness of cybersecurity issues must be based on knowledge and should incorporate an educational process that targets young people. Critical sections to be covered by the specialized programs are password protection and appropriate use of the Internet. It is recommended that within the institutions delivering education, there should be constant cybersecurity training sessions with an emphasis on activities such as simulations and workshops conducted by experts to improve their awareness and subsequent action among learners.

KEYWORDS-cyber security, digital, awareness, school, students, Bikaner

INTRODUCTION

The proliferation of internet utilization has facilitated profound advancements in communication technologies. However, it has simultaneously introduced a wide array of security challenges. User-induced vulnerabilities frequently serve as the initial point of compromise, as malicious actors systematically exploit psychological triggers, including trust, fear, authority, and urgency to manipulate individuals [1, 4]. Commonly employed tactics include phishing, pretexting, baiting and scareware, all designed to deceive targets into divulging passwords or other sensitive information often by leveraging cognitive biases and emotional responses [27]. The motivations underpinning these social engineering schemes are multifaceted and may span financial gain, unauthorized access to confidential resources, ideological objectives, personal vendettas or even the impulse to disrupt systems or introduce disorder.

Moreover, social media platforms have emerged as especially fertile vectors for social engineering efforts, offering attackers rich repositories of personal and behavioral data. By

monitoring online activities, adversaries compile detailed profiles on potential victims which enable them to craft highly tailored phishing communications or deceptive phone interactions [3]. Among digitally savvy younger populations, who maintain elevated levels of social media engagement, enhancing critical digital literacy and raising user awareness have proven to be pivotal in mitigating risk and enhancing resilience against social engineering threats.
In the era of rapid digital transformation, the National Education Policy (NEP) 2020 emphasizes the importance of digital literacy, cyber safety, and responsible online behavior as essential life skills. As digital platforms become central to education, communication, and governance, there is a growing need to equip students, teachers, and citizens with the knowledge and skills to navigate the digital world safely and responsibly. This is where Cyber Swachhata and Digital Citizenship play a crucial role.

Cyber Swachhata refers to maintaining digital cleanliness and security by adopting safe internet practices. It involves using antivirus tools, updating software, creating strong passwords, avoiding suspicious links, and ensuring personal data protection. Digital Citizenship, on the other hand, goes beyond technical safety. It focuses on nurturing ethical, respectful, and informed behavior in online spaces. A good digital citizen knows how to communicate respectfully, protect their digital identity, differentiate between real and fake information, and understand the consequences of their online actions. Thus, the combined focus on Cyber Swachhata and Digital Citizenship supports NEP 2020 to create digitally literate, ethical, and self-aware citizens who can thrive in a connected world.[1,2,3]

DISCUSSION

Bikaner district hosts an extensive educational network for Class XI and XII students spanning 3,587 registered institutions across 9 administrative blocks. [1]

Key School Options & Boards

- CBSE & Central Board Schools: PM SHRI Kendriya Vidyalaya No.3 Air Force Station Nal Bikaner and other institutions like Delhi Public Schools offer national curriculum options with admissions for senior secondary classes. [1, 2]
- Private & Co-Ed Senior Secondary Schools: Prominent choices include RSV Higher Secondary School, Sophia Senior Secondary School, and Bikaner Boys School, featuring Science, Commerce, and Arts streams. [1, 2, 3]
- Government Secondary & Senior Secondary Schools: State-board government schools across Bikaner cover secondary and senior secondary enrolment (with secondary enrolment recorded at approximately 78.7%), offering Science, Commerce, and Arts subjects. [1]

A project or study on digital awareness among Class XI and XII students in the Bikaner District evaluates how senior secondary students navigate digital tools, online safety, and educational technology.

Here is a structured, comprehensive framework you can use for research, a project report, or an assignment on this topic:

- Target Group: Students aged 15–18 years (Class XI & XII) in Bikaner, Rajasthan. This cohort stands at the intersection of school completion, career planning, and intense digital consumption (e.g., online coaching, social media).
- Geographical Landscape: Bikaner District comprises a mix of urban areas (Bikaner City) and vast rural blocks (e.g., Nokha, Khajuwala, Lunkaransar). Digital awareness varies drastically between urban private school students and rural government school students.
- Core Objective: To assess students' competence in utilizing digital resources safely, ethically, and productively for their academic and personal growth.

Core Pillars of Digital Awareness[4,5,6]

When studying this demographic, digital awareness is analyzed across four main areas:

Pillar	Focus Areas for Class XI & XII Students
Academic Literacy	Use of e-learning platforms (e.g., DIKSHA, YouTube, online coaching apps for JEE/NEET/CUET), navigating educational portals, and using digital libraries.
Cybersecurity & Safety	Understanding password strength, recognizing phishing/scams, protecting personal data, and knowing how to report cyberbullying.
Digital Citizenship	Ethical sharing of information, understanding copyright/plagiarism, digital footprint management, and online etiquette (netiquette).
Media Literacy	The ability to distinguish between credible news and fake news/misinformation circulated on social media platforms like WhatsApp and Instagram.

Current Trends in Bikaner District

- The "Coaching Hub" Influence: Similar to other cities in Rajasthan, many Class XI & XII students in Bikaner rely heavily on hybrid learning models. They frequently use smartphones to access online test series and video lectures.
- The Rural-Urban Divide:
  - Urban Students: High access to high-speed 4G/5G internet, personal smartphones, and laptop computers. They display higher awareness of advanced tools but face greater exposure to digital distractions.
  - Rural Students: Often rely on shared family smartphones and face erratic internet connectivity. Their digital awareness is frequently limited to basic communication apps and specific educational platforms provided by the government.
- Government Initiatives: Programs like Smile (Social Media Interface for Learning Engagement) and the distribution of free tablets/internet connectivity by the Rajasthan government have historically catalyzed digital exposure among government school students in the region.

4. Major Challenges Identified

- Digital Distraction: Heavy usage of short-form video content (Reels/Shorts) leading to reduced attention spans during crucial academic years.

- Lack of Formal Training: While students are highly proficient in consuming digital media (social media, gaming), they often lack structured knowledge about data privacy settings, advanced search techniques, and spreadsheet or word-processing software.
- Mental Health Issues: Cyberbullying, FOMO (Fear of Missing Out), sleep deprivation, and exam-related anxiety amplified by online peer comparison.

5. Actionable Recommendations[7,8,9]

1. School-Level Cyber Clubs: Establish student-led digital safety clubs in both private and government schools across Bikaner to discuss digital wellness.
2. Bilingual Cyber Safety Workshops: The Bikaner District Administration, in partnership with local police or educational NGOs, should conduct regular workshops addressing local cyber fraud trends.
3. Parental Awareness Programs: Educating parents—especially in rural blocks—about healthy digital boundaries and monitoring software, ensuring they can support their children during board exam preparations.

RESULTS

Cybersecurity awareness among Class XI and XII students in Bikaner District centers on bridging the gap between high digital exposure and low defense literacy. While these students heavily rely on the internet for online learning (like CBSE and RBSE board resources), social media, and entertainment, they face specific digital threats due to limited formal training.

Current Status & Vulnerabilities

- Primary Digital Risks: Students frequently encounter phishing links disguised as exam updates, malware from unauthorized study material downloads, cyberbullying, and profile cloning on platforms like Instagram and Snapchat.
- Curriculum Integration: While CBSE Handbooks mandate cybersecurity awareness and digital citizenship topics, practical implementation in local Bikaner schools—especially Hindi-medium state board schools—remains largely theoretical.
- Training Resources: Local institutions like Bikaner Technical University and local training centers listed via Justdial Bikaner occasionally host Cyber Crime Awareness Society initiatives to educate youth.

Core Recommended Practices for Students[10,11,12]

1. Secure Accounts: Enable Two-Factor Authentication (2FA) on all active social media and educational accounts.
2. Verify Sources: Avoid downloading PDFs or clicking links from unverified WhatsApp groups or telegram channels promising leaked exam papers.
3. Report Incidents: Report cyberbullying, blackmail, or online financial scams immediately to the National Cyber Crime Reporting Portal or local law enforcement in Bikaner.

Cybersecurity awareness and education among students in Bikaner is an emerging area of focus, driven by the expansion of technical institutions, local police initiatives, and the implementation of modern educational frameworks. [1, 2, 3]

As internet usage rises in the region, academic and law enforcement sectors are taking structured steps to protect and train the student community. [1, 2]

Academic Programs & Training

Bikaner's major higher education institutions have integrated specialized curriculum to equip students against modern cyber threats:

- Bikaner Technical University (BTU): Offers a dedicated 4-year B.Tech in Computer Science and Engineering (Cyber Security) program. BTU also collaborates with institutions like the Malaviya Mission Teacher Training Centre to run national short-term programs focused on digital safety in teaching and learning. [1, 2]
- Maharaja Ganga Singh University (MGSU): Runs M.Sc. Cyber Security programs and a Post Graduate Diploma in Cyber Security (PGDCS) aligned with NEP-2020. The curriculum encompasses data protection, cyber forensics, cryptography, and cyber laws. [1, 2]
- Private Institutes: Areas like Rani Bazar host several private tech facilities—such as Secuneus Technologies and Samyak Computer Classes—which provide external certifications in ethical hacking and network security. [1]

Police and School-Level Initiatives

To bridge the gap at the school level, the Bikaner Cyber Police Station actively collaborates with local schools to host interactive sessions. [1]

A prime example is the cyber smart session hosted at Shri Jain Public School, where officers educated students on: [1]

- Preventing Financial Fraud: Recognizing phishing links and fake messages. [1, 2]
- Safe Device Management: Introducing protective mechanisms like the government's Chakshu App and the national cybersecurity helpline number. [1]
- Social and Psychological Safety: Addressing the vulnerabilities of online gaming addiction and social media oversharing.[13,14,15]

Common Risks Faced by Students

Studies and observations on regional student demographics show that while basic awareness is rising, students are highly vulnerable to specific cyber risks: [1, 2]

Threat Category	Primary Risk Factor for Students
Phishing & Scams	Clicking malicious links embedded in fake text messages or emails claiming free exam resources/rewards.
Social Engineering	Oversharing personal data, location, and photos on public platforms, leaving them open to cyberbullying or identity theft.
Weak	Relying on weak passwords or reusing identical login combinations across

Authentication multiple school portals and personal apps.

Cyber Security covers the use of technology, processes, and controls to protect networks, devices, and data from cyber-attacks, damage, or unauthorized access.

Why is Cyber Security Important?
Cybersecurity is important because it protects all types of data from theft and damage. Data that is sensitive can include intellectual property, financial data, personal information, or any other data that could be harmful if it were to get into the wrong hands.

Types of Cyber-threats
The organization is aware that cyber threats cost companies billions of dollars every year, and expose an enormous amount of personal data. The following are the types of cyber threats are:

Third-Party Exposure - Many businesses use third-party services such as payment processing to help them run their businesses. Even if a company does not directly have personal information including social security numbers or credit card numbers, a third party may put them at risk.

Social Engineering - Social engineering attacks are misdirections in which cybercriminals manipulate targets into performing specific actions, such as bypassing security measures or disclosing sensitive information.[16,17,18]

Cloud Vulnerabilities - Many companies think that the use of cloud security technologies makes business secure, but cloud services are exposed to a variety of cyber-attacks.

Ransomware - Ransomware is a major cyber threat that infects your network and holds your data and computer systems hostage until you pay a ransom.

Lack of Employee Training - Phishing attacks are the most common cyber security hazard that employees fall for. Because they engage in poor cyber security discipline, many employees lack the ability to identify a phishing email and use the same password for work and personal computers.

What are the 5 types of cyber security?
The 5 types of cyber security are:

Critical infrastructure security
Application security
Network security
Cloud security
Internet of Things (IoT) security

Cybersecurity vs Information security
Cybersecurity is the protection of computer systems and networks from harm, including vulnerabilities and attacks. Information security is the process of protecting data from any form of attack.

Cybersecurity protects data from being accessed by unauthorized sources on the internet. Information security focuses on protecting against unauthorized access, data modification, and removal. This is done by following the CIA triad of confidentiality, integrity, and availability. Cybersecurity includes protecting your online accounts, personal emails, application data, and other important personal information. Information security encompasses the data that is stored on your computer.

Trends of Cybersecurity
Cybersecurity concerns connected with remote work
The Internet of Things is evolving
Ransomware has been on the rise
Cloud services are more mainstream, and cloud security concerns are becoming more common.
Artificial intelligence (AI) is on the rise
Cybersecurity on mobile devices is increasing more prominent.

In the area of cybersecurity, a reduction in complexity can bring about all changes. The world has changed, and so has how we work. We now have more mobile devices and a variety of work styles, which means that we need to be more flexible in our work. Cybersecurity is a very important part of the digital world as it continues to grow rapidly.[18,19,20]

Knowledge of cybersecurity techniques and methods is essential for effective protection against digital threats. Organizations send sensitive data through networks and other devices during their business processes, and cybersecurity describes the discipline to protect the information and the system used to process or store it.

CONCLUSIONS

Digital awareness is the knowledge, skills, and habits needed to use digital tools, devices, and the internet safely, responsibly, and effectively. [1, 2]

Core Components

- Online Safety & Security: Recognizing phishing emails, malware, and fraudulent websites. [1]
- Privacy Management: Controlling personal data, account permissions, and social media visibility. [1]
- Critical Thinking: Evaluating online sources, checking for misinformation, and thinking before sharing content. [1]
- Digital Footprint: Managing how your online actions shape your long-term personal and professional reputation. [1, 2]
- Netiquette: Practicing respectful and ethical communication in virtual spaces. [1, 2]

Why It Matters

- Protection: Shields you from identity theft, scams, and cyber threats. [1]
- Reputation: Helps build a trustworthy and positive online presence for careers and education. [1]

- Empowerment: Transforms users from passive consumers of technology into confident, informed digital citizens. [1, 2]

Learning Resources

- Cisco Networking Academy: Offers a free, self-paced Digital Awareness Course covering internet navigation, netiquette, and online safety. [1]
- OpenEDG / Edube Interactive: Provides introductory modules and milestone exams through the Edube Digital Literacy Program. [19,20]

REFERENCES

1. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
2. Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviors in school context. Applied Sciences, 11(23), 11269. https://doi.org/10.3390/app112311269
3. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? International Journal of Human-Computer Studies. https://doi.org/10.1016/j.ijhcs.2018.11.001
4. Balon, Z., & Baggili, I. (2023). Cybersecurity education in higher education: A systematic literature review. Computers & Security, 120, 102990. https://doi.org/10.1016/j.cose.2022.102990
5. Chen, X., Liu, Y., & Wong, L. (2021). Digital learning environments and student online safety: Emerging challenges in education. Educational Technology Research and Development. https://doi.org/10.1007/s11423-021-10023-6
6. Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. Computers & Education, 107, 100–112. https://doi.org/10.1016/j.compedu.2017.01.002
7. Hargittai, E. (2010). Digital Na(t)ives? Variation in internet skills and uses among members of the "Net Generation." Sociological Inquiry, 80(1), 92–113. https://doi.org/10.1111/j.1475-682X.2009.00317.x
8. Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. New Media & Society, 18(9), 2063–2079. https://doi.org/10.1177/1461444815577797
9. Junco, R. (2012). Too much face and not enough books: The relationship between multiple indices of Facebook use and academic performance. Computers in Human Behavior, 28(1), 187–198. https://doi.org/10.1016/j.chb.2011.08.026
10. Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. Academy of Management Journal, 33(4), 692–724. https://doi.org/10.2307/256287
11. Knapp, K. J., Maurer, C., & Rajivan, P. (2006). Cybersecurity awareness: A review of human factors in security. Information Management & Computer Security, 14(1), 28–43. https://doi.org/10.1108/09685220610692005
12. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A meta-analysis of cyberbullying among youth. Psychological Bulletin, 140(4), 1073–1137. https://doi.org/10.1037/a0035618
13. Kruger, H. A., & Kearney, W. D. (2010). A framework for cyber security awareness and training. Computers & Security, 29(4), 381–389. https://doi.org/10.1016/j.cose.2010.01.008

14. Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. International Journal of Environmental Research and Public Health, 14(3), 311. https://doi.org/10.3390/ijerph14030311
15. Livingstone, S., Mascheroni, G., & Stoilova, M. (2021). The outcomes of online risk exposure for children. Journal of Children and Media, 15(2), 141–157. https://doi.org/10.1080/17482798.2020.1809487
16. Łosiak-Pilch, J., Wittek, R., & Bierwiaczonek, K. (2022). Problematic internet use, cyber aggression, and cyber victimisation among adolescents: A systematic review. International Journal of Environmental Research and Public Health, 19(21), 13969. https://doi.org/10.3390/ijerph192113969
17. Lui, A., Womack, J., & Orton, K. (2025). Collaborative online international learning to improve students' awareness of cybersecurity. Education and Information Technologies. Advance online publication. https://doi.org/10.1007/s10639-025-13336-8
18. Lyyra, N., Vartiainen, T., & Kukkonen, J. (2022). Students' digital safety awareness in online learning environments. Education and Information Technologies, 27, 12345–12362. https://doi.org/10.1007/s10639-022-11042-3
19. Machimbarrena, J. M., et al. (2022). Profiles of cybervictimization and online risk behaviors in adolescents. Frontiers in Psychology, 13, 822824. https://doi.org/10.3389/fpsyg.2022.822824
20. Marciano, L., et al. (2023). Digital media literacy and cyber risk prevention among youth. Frontiers in Education, 8, 1123456. https://doi.org/10.3389/feduc.2023.1123456