

Cyber Safety, Digital Wellbeing and Media Literacy for Students: Towards a Safety Framework for Aspiring India

Kalyan Kumar¹, Magnum Sharma²

^{1,2}Research Scholar, Department of Teacher Education, Central University of Haryana, ORCID:

Abstract

Cyber safety refers to the practices adopted in the digital world for developing safe and sound habits that protect an individual's identity, privacy and devices from threats in the digital environment. The wellbeing of persons in the digital space has a direct bearing on their productivity at the workplace and on their overall progress.

As the digital space becomes an alternative workstation where students learn and explore in the process of knowledge building, the risk of vulnerability appears inevitable. A growing sense of awareness is now observed among students; however, in this data-driven age, the scale of vulnerability has increased considerably, and an existing gap continues to widen, underlining an urgent requirement for a cybersecurity and safety framework for Aspiring India.

The digital revolution, shaped by inexpensive mobile internet, has transformed the educational landscape of India; yet students face escalating threats to their personal identity, privacy and devices. There is an urgent need to bridge these safety concerns and to develop wellbeing strategies that safeguard the aspiring minds of India in their path of digital knowledge building.

Based on recent empirical studies, the National Crime Records Bureau's official 'Crime in India 2024' report released in May 2026 [7], and Haryana state enforcement data through June 2026 [2, 10], this paper focuses on the scale of the problem, reviews the current state of student cyber-safety awareness in India, identifies the structural gaps behind it, and proposes a three-pillar framework — “Awareness, Behaviour and Institutional Support” — for building sustainable digital wellbeing among citizens.

Keywords: Cyber safety, Media literacy, Aspiring India, Internet Safety Framework, Digital wellbeing

1. Introduction

India's education system is undergoing a rapid digital transformation. Over the period, the availability of cheap internet and cost-efficient smartphones has turned over the digital world into an alternative classroom model, where students learn, construct and explore learning beyond the physical boundaries of a school or college. This shift, often regarded as a strong symbol of 'Digital India' and an 'Aspiring India' moving towards a knowledge-based economy, has also opened a parallel and less-discussed frontier: the exposure of young, often first-generation internet users, to a fast-growing range of digital threats which positions them more vulnerable.

Cyber safety refers to the practices and habits adopted to protect one's identity, privacy and devices from threats that exist in the digital world. It is widely linked to the broader idea of digital wellbeing — the

sense of psychological and informational safety that allows a person to be productive and to progress in a workspace that is increasingly virtual. For students, whose digital literacy is still developing alongside their academic literacy, the absence of structured cyber safety education leaves a widening gap between the pace of digital adoption and the pace of digital readiness.

This paper examines the current landscape of cyber safety awareness among Indian students, presents a quantitative analysis of recent national data and survey findings, and proposes a practical framework through which schools, colleges and policymakers can build media literacy and digital wellbeing into the everyday learning process.

2. The Digital Landscape of Indian Students

The rapid decline in mobile data costs has been among the biggest drivers of internet adoption in India, extending connectivity into small towns and rural areas that previously had limited digital access. For students, this has meant near-constant access to search engines, social media, messaging platforms and AI-based learning tools. Digital access is no longer restricted to computer laboratories or scheduled periods; it is now embedded in daily academic and social life.

This same accessibility, however, has outpaced the institutional structures meant to guide its safe usage. As the data presented in this paper shows, both the volume of cybercrime and its impact on young users have grown sharply in the most recent reporting period, forming the backdrop against which student vulnerability must be understood.

3. Literature Review

A growing body of Indian research has begun to document the gap between digital access and digital safety competence among students. A 2025 survey of middle and secondary level students found that awareness of safe internet practices was low overall, and notably lower among younger students in the 12–15 age group compared with those aged 15–18, pointing to the need for age-appropriate cyber safety instruction rather than a uniform, one-size-fits-all approach (Panjani et al., 2025) [8].

Similar patterns emerge at the undergraduate level. A survey of undergraduate students in a tribal-dominated district of western Odisha found that most respondents fell in the average-to-above-average awareness range, with urban students scoring only marginally higher than rural students; the study recommended integrating structured cyber-safety modules into the undergraduate curriculum and running regular awareness programmes, treating the issue as one of curriculum design rather than isolated messaging or geography alone (Sahu et al., 2026) [9].

A study of cybercrime awareness among higher-education students in Haryana, covering 500 students drawn from both professional and traditional (non-professional) courses and assessed using the standardised Cybercrime Awareness Scale (CCAS-RS), found that professional-course students demonstrated significantly higher cybercrime awareness than their peers in traditional courses, with no significant difference by gender; however, awareness across the sample fell only in the 'average' category rather than the high range (Choudhary, 2020) [1]. A related study of 240 teacher trainees from Haryana similarly found comparatively moderate awareness levels, with significant effects of gender and locality (Malhotra et al., 2017) [5]. Taken together with the Odisha finding above, this suggests that course type and institutional stream — not just gender or urban/rural location — shape how much cyber safety knowledge students acquire, pointing to curriculum design, not just geography, as a variable for closing the gap.

A separate empirical study of 150 college students found that although a majority were broadly aware of cybercrime, only a minority who had personally experienced a cybercrime incident reported it to the authorities, citing a lack of trust, unfamiliarity with reporting procedures, or reluctance to file a formal complaint — indicating that the awareness gap extends beyond prevention into response and recourse (Hamsaveni, 2025) [4].

On the intervention side, industry-led programmes provide evidence of what structured training can achieve. A cyber-safety skilling initiative implemented across 40 schools in Maharashtra and Tamil Nadu, reaching more than 10,000 students, parents and educators, reported a substantial increase in participants' cyber safety knowledge following training, suggesting that even relatively short, structured interventions can produce measurable gains when they are designed around clear learning outcomes (Gen/Norton et al., 2024) [3].

Taken together, the literature suggests three findings: (i) cyber safety awareness among Indian students is generally low-to-moderate and uneven across age groups and regions; (ii) awareness gaps persist regardless of gender or locality, indicating a systemic rather than a demographic issue; and (iii) structured, curriculum-embedded interventions can meaningfully improve awareness, but current efforts remain fragmented, localised and largely dependent on individual institutions or external partners rather than on a coordinated national framework.

4. Statement of the Problem

Despite growing recognition of the issue, India does not yet have a unified, curriculum-embedded cyber safety and digital wellbeing framework for students. Existing efforts appear to be a reactive response to cybercrime after it occurs, rather than a precautionary one, and they tend to be concentrated in urban centres and better-resourced schools, leaving rural and semi-urban students, who now form a large share of India's new internet users, comparatively underserved. This paper treats these as the central gaps to be addressed.

5. Objectives of the Study

- To examine the current state of cyber safety and digital wellbeing awareness among students in India.
- To quantitatively analyse recent national cybercrime data and survey findings to establish the scale and pattern of the problem.
- To propose a practical, scalable framework integrating awareness, behavioural practice and institutional support for student cyber safety.

6. Research Methodology

6.1 Research Design

This study follows a descriptive-analytical research design based entirely on secondary data. Rather than collecting new primary data through a fresh survey or fieldwork, the study synthesises existing peer-reviewed research, official administrative crime statistics and programme-evaluation reports to build a composite, evidence-based picture of student cyber safety in India, and to derive a practical framework from the patterns observed across these sources. This design was chosen to establish the scale of the problem and identify structural gaps across the existing evidence base, rather than to test a specific hypothesis about a single population.

6.2 Data Sources and Selection Criteria

Three categories of secondary data were drawn upon.

- Administrative and official statistics: the Ministry of Home Affairs / Indian Cyber Crime Coordination Centre (I4C) portal-complaint data (2024–2025) [6], the National Crime Records Bureau's annual 'Crime in India' reports (2018–2022 editions and the 2024 edition released in May 2026) [7], and Haryana state government / Haryana Police enforcement data (January 2025–June 2026) [2, 10].
- Peer-reviewed academic studies: descriptive and survey-based research on student and youth cybercrime awareness published in Indian academic journals between 2020 and 2026, covering Haryana, Odisha and Tamil Nadu [1, 4, 5, 8, 9].
- Programme and industry reports: a monitoring-and-evaluation report from a structured, multi-school cyber-safety skilling initiative (Gen/Norton et al., 2023–2024) [3].

Sources that could not be traced to an identifiable original publication were used only for general qualitative context in the Literature Review.

6.3 Analytical Approach

Two complementary analytical methods were used. First, a thematic synthesis of the literature review sources was conducted to identify recurring patterns across independent studies. Second, a descriptive quantitative analysis was applied to the administrative and programme-report data, presenting the underlying figures as charts accompanied by a structured interpretation of what each pattern implies for student cyber safety.

6.4 Delimitations of the Study

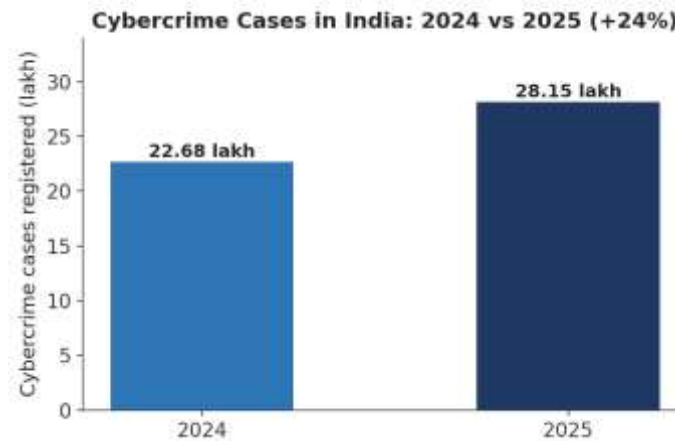
- This is a secondary-data, desk-based study; no new primary survey, interview or experimental data was collected specifically for this paper.
- The evidence base is heterogeneous in scale and geography, ranging from national administrative data to single-institution surveys.
- Because the underlying studies were not conducted using a common instrument or sampling frame, no attempt is made to statistically pool or re-test their findings; percentages and figures are reported as published by the original sources.
- The proposed A-B-I framework is conceptual, derived from patterns in the reviewed evidence rather than from a piloted intervention; it outlines the empirical pilot study that would be needed to validate it directly.

7. Data Analysis and Interpretation

This section presents a quantitative picture of the cyber safety landscape for Indian students, drawing on national cybercrime statistics (Ministry of Home Affairs / Indian Cyber Crime Coordination Centre data as reported in 2025–26 policy and industry sources [6], and the NCRB's official 'Crime in India 2024' report, released in May 2026 [7]), state-level enforcement data from Haryana through mid-2026 [2, 10], and recent peer-reviewed survey research. Each figure is accompanied by an interpretation of its implications for student cyber safety and for the framework proposed in Section 9.

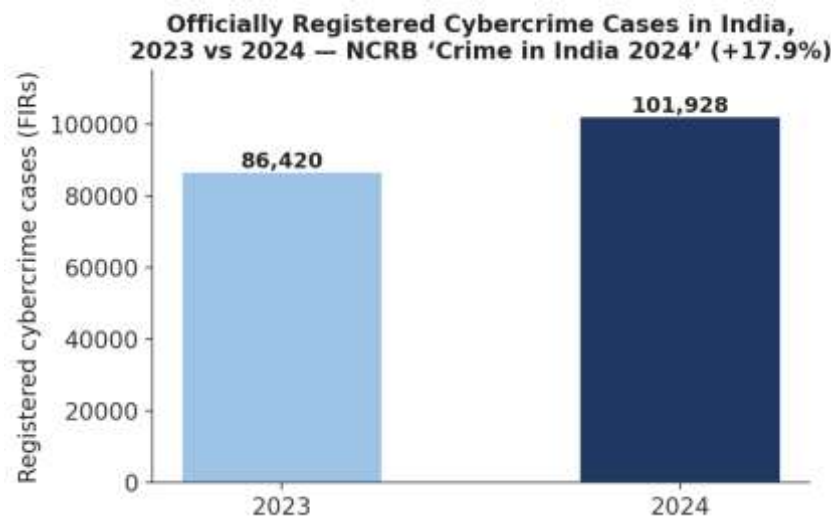
7.1 Scale and Growth of Cybercrime in India

Figure 1. Cybercrime-Related Complaints Received on India's National Cybercrime Reporting Portal, 2024 vs 2025



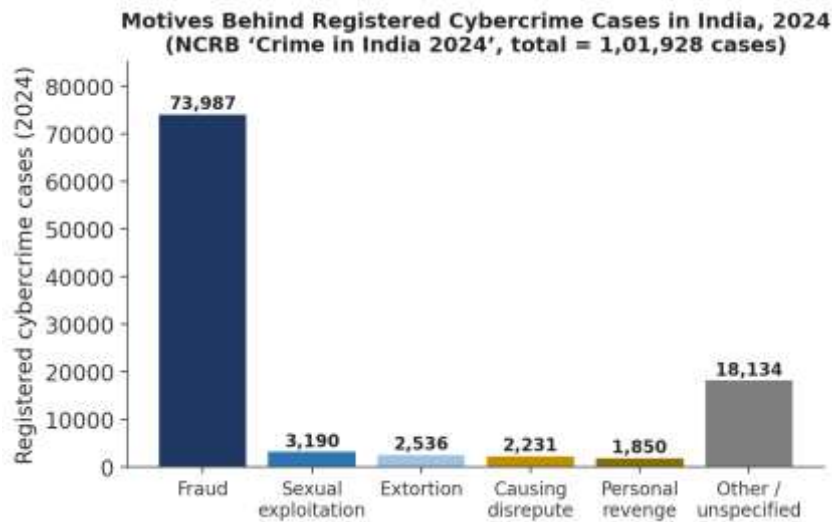
Portal-level complaints rose from approximately 22.68 lakh in 2024 to 28.15 lakh in 2025, an increase of nearly 24 percent in a single year [6]. This growth rate significantly outpaces the growth of internet users over the same period, indicating that the digital threat environment is intensifying faster than the general expansion of digital access.

Figure 2. Officially Registered Cybercrime Cases (FIRs) in India, 2023 vs 2024 — NCRB 'Crime in India 2024' Report, Released May 2026



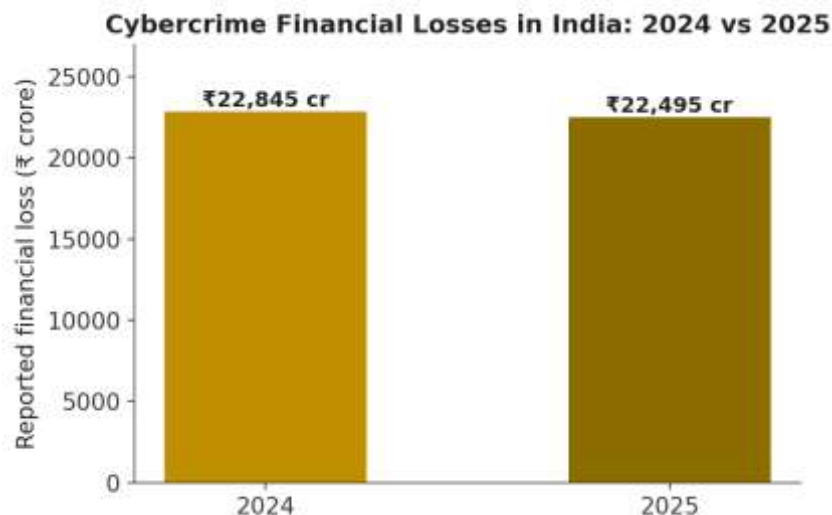
India's own crime-records authority confirms the same trend through a different, more conservative lens: officially registered cybercrime cases (as opposed to portal complaints, which include unverified reports) rose from 86,420 in 2023 to 1,01,928 in 2024 — a 17.9 percent increase that pushed registered cybercrime past the one-lakh mark for the first time on record [7]. The national cybercrime rate rose correspondingly from 6.2 to 7.3 cases per lakh population, even as India's overall registered crime rate fell by 6 percent over the same period.

Figure 3. Motives Behind Registered Cybercrime Cases in India, 2024 (NCRB 'Crime in India 2024')



Fraud accounts for nearly 73 percent of all registered cybercrime cases in India (73,987 of 1,01,928), followed by sexual exploitation, extortion and reputational-harm motives combined [7]. For a student population that is increasingly financially independent — managing UPI payments, part-time earnings and scholarship transfers — this concentration of fraud-motivated cybercrime makes financial-literacy-adjacent cyber safety training (recognising phishing, fake investment schemes and 'digital arrest' frauds) a particularly high-leverage curriculum component.

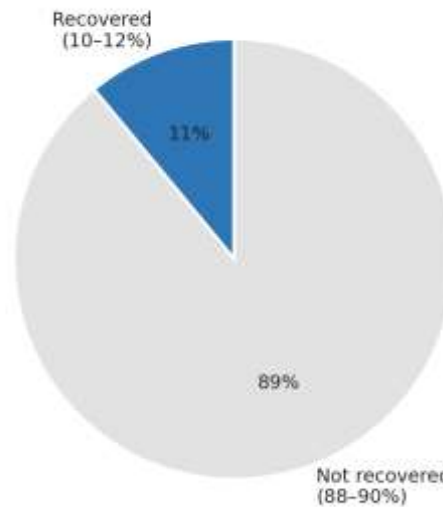
Figure 4. Reported Financial Losses to Cybercrime in India, 2024 vs 2025



Financial losses remained almost flat (₹22,845 crore in 2024 versus ₹22,495 crore in 2025) even as portal complaint volumes rose by 24 percent, implying a fall in average loss per case [6]. This is consistent with a shift towards high-volume, lower-value frauds and improved real-time fund-blocking by banks and law enforcement — but it also means more individual victims overall, a pattern that has direct relevance for a large, first-time-user population such as students.

Figure 5. National Recovery Rate of Funds Lost to Cybercrime

National Recovery Rate of Stolen Cybercrime Funds

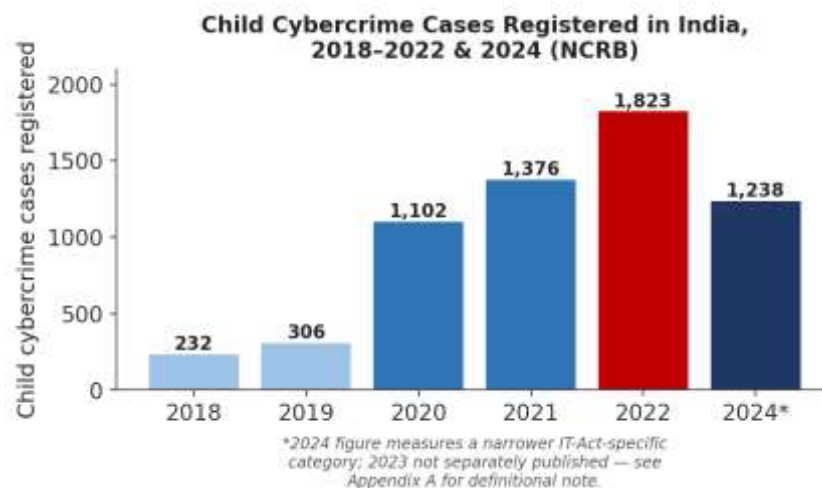


Only 10–12 percent of stolen funds are recovered nationally [6], underscoring that prevention and early recognition of threats — the core aims of cyber safety education — are far more effective levers than post-incident recovery. For students with limited financial resources, this low recovery rate raises the practical stakes of awareness gaps considerably.

7.2 Child and Youth Cybercrime: A Detailed Breakdown

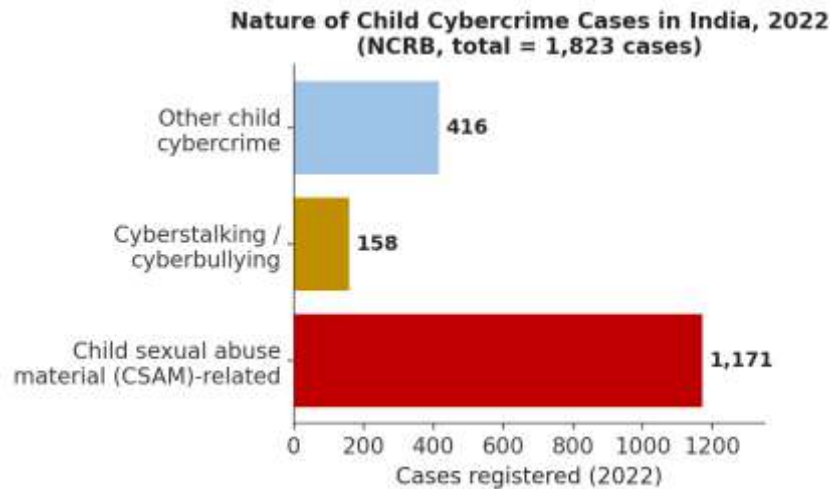
Because national totals can obscure how cybercrime specifically affects children and young people, this section presents the NCRB's child-cybercrime data across two dimensions: its trend over time and the composition of what these cases involve [7].

Figure 6. Child Cybercrime Cases Registered in India, 2018–2022 and 2024 (NCRB)



Child cybercrime cases rose steeply from 232 in 2018 to 1,823 in 2022 — nearly an eightfold increase in four years — before the NCRB's 2024 report recorded 1,238 cases under a narrower, IT-Act-specific measure of child cybercrime (see the definitional note in Appendix A.2) [7]. Even allowing for this change in how the category is measured, the multi-year trend confirms that children have gone from a marginal share of cybercrime victims to a substantial and fast-growing one, reinforcing the case for age-specific, school-embedded cyber safety education rather than generic public awareness campaigns alone.

Figure 7. Nature of Child Cybercrime Cases in India, 2022 (NCRB, Total = 1,823 Cases)

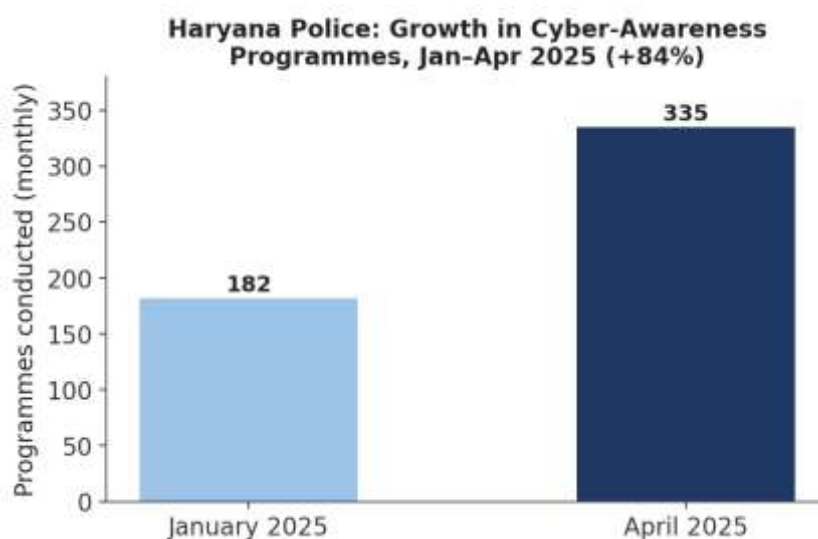


Within child cybercrime cases, 1,171 of 1,823 (64 percent) involved child sexual abuse material, with cyberstalking/cyberbullying (158 cases) and other offences (416 cases) making up the remainder [7]. The NCRB's 2024 report echoes this composition at the newer, narrower count: 1,099 of 1,238 IT-Act cybercrime cases against children (89 percent) involved sexually explicit content. Both datasets point to the same conclusion — that content-based exploitation, not just fraud or bullying, is the dominant form of cybercrime harm facing children in India, which has direct implications for what 'identity and privacy protection' content should emphasise in the Awareness pillar proposed in Section 9.

7.3 Regional Case Study: Haryana's Cyber-Safety Response

Haryana offers a useful state-level case study because it combines an active, recently reported institutional response with independent academic survey evidence on student awareness, allowing the two to be read side by side.

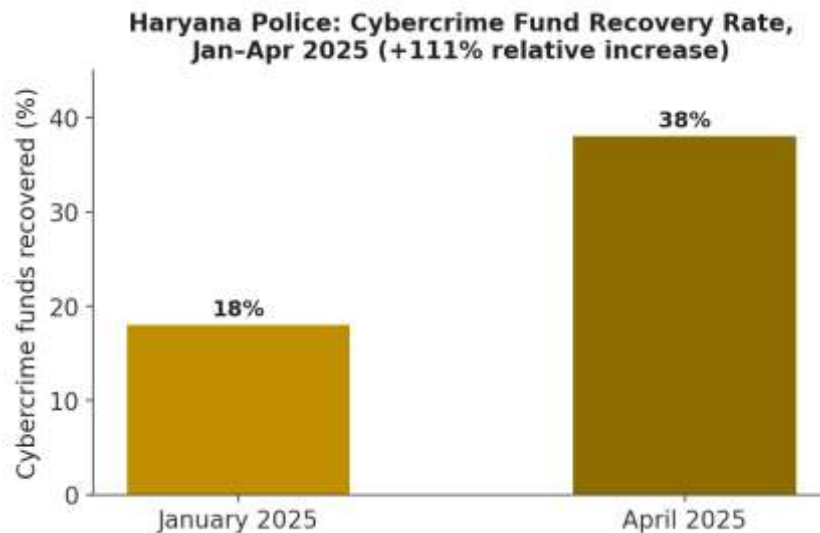
Figure 8. Growth in Cyber-Awareness Programmes Conducted by Haryana Police, January–April 2025



Haryana Police nearly doubled its monthly cyber-awareness programme count, from 182 in January 2025 to 335 in April 2025 (an increase of roughly 84 percent), with citizen participation in these programmes rising from about 45,920 to 67,144 over the same period (a 46 percent increase) [10]. This indicates a

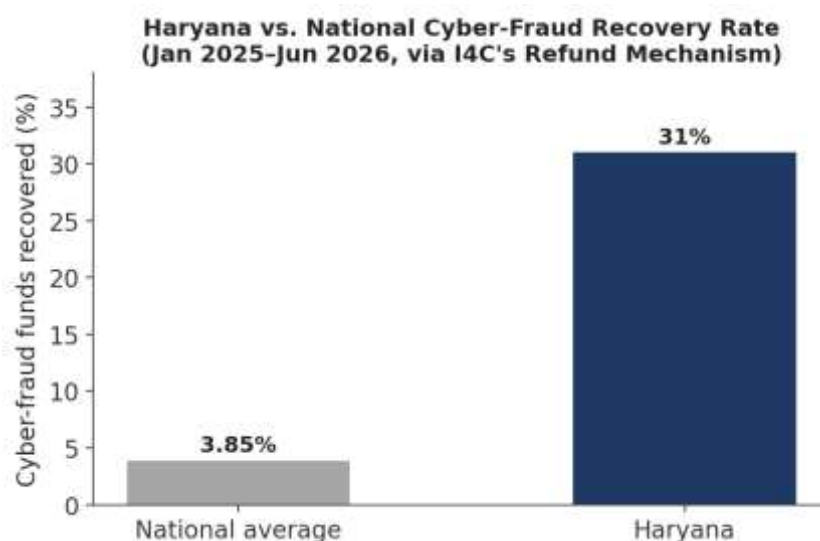
genuine, recent scale-up of outreach specifically targeting schools, colleges and community institutions in the state — the same population this paper is concerned with.

Figure 9. Cybercrime Fund Recovery Rate in Haryana, January–April 2025



Over the same four-month window, Haryana's cybercrime fund recovery rate more than doubled, from 18 percent to 38 percent, alongside a 6.6-fold increase in fraud-linked mobile numbers blocked and a 9-fold increase in IMEI blacklisting [10]. This indicates that Haryana's recent enforcement gains are real and measurable, but a recovery rate of 38 percent, even after improvement, still means majority of stolen funds are not recovered, reinforcing that prevention-focused cyber safety education remains more valuable than post-incident recovery for a student population with limited financial cushion.

Figure 10. Haryana vs. National Cyber-Fraud Recovery Rate, January 2025–June 2026 (via I4C's Multi-Agency Refund Mechanism)



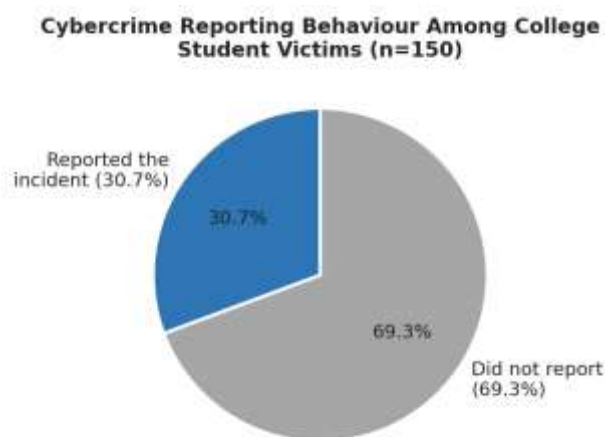
The most recent available data — covering January 2025 through June 2026 — shows Haryana sustaining a 31 percent cyber-fraud recovery rate against a national average of just 3.85 percent, more than eight times higher [2]. Over this window, Haryana Police also arrested 3,947 cybercriminals in the first half of 2026 alone, trained roughly 9,100 personnel in cybercrime investigation, and removed 14,139 pieces of

illegal online content via the Sahyog Portal. This confirms that Haryana's cyber-enforcement scale-up begun in 2025 has been sustained, not just a short-term spike — which strengthens the case that enforcement capacity in the state is now outpacing measured student awareness gains.

Set against this institutional momentum, the academic evidence on Haryana student awareness is more sobering: the Choudhary (2020) [1] study of 500 higher-education students found overall awareness in only the 'average' category, with a clear gap between professional-course and traditional-course students. These two strands of evidence suggest that Haryana's enforcement and outreach infrastructure is scaling up faster than the underlying awareness levels of its student population — exactly the kind of gap the institutional-support pillar of the framework is designed to close.

7.4 Student Reporting Behaviour

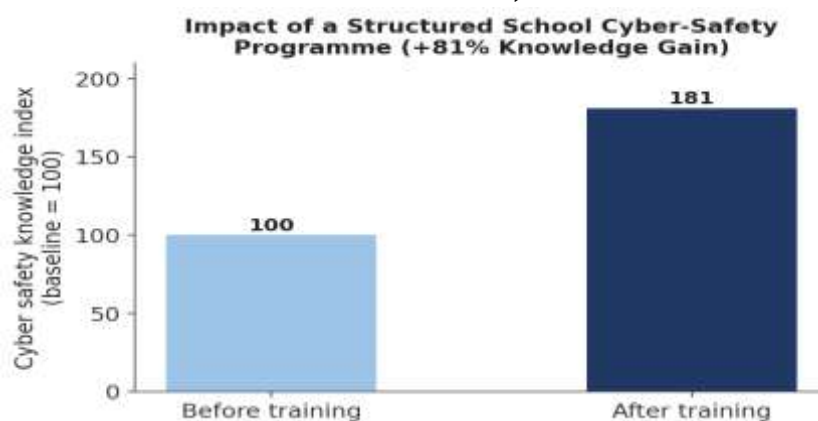
Figure 11. Reporting Behaviour among College Student Victims of Cybercrime (n = 150)



Among students who had personally experienced a cybercrime incident, 69.3 percent did not report it to authorities, most commonly citing a lack of trust or unfamiliarity with reporting procedures (Hamsaveni, 2025) [4]. This points to a second, distinct gap beyond preventive awareness: students who are victimised often lack the confidence or knowledge to pursue redress, which likely under-counts the true scale of student-targeted cybercrime in official statistics, and points to a need for clearer, more accessible reporting pathways within educational institutions themselves — including in states like Haryana where awareness-programme reach is already expanding.

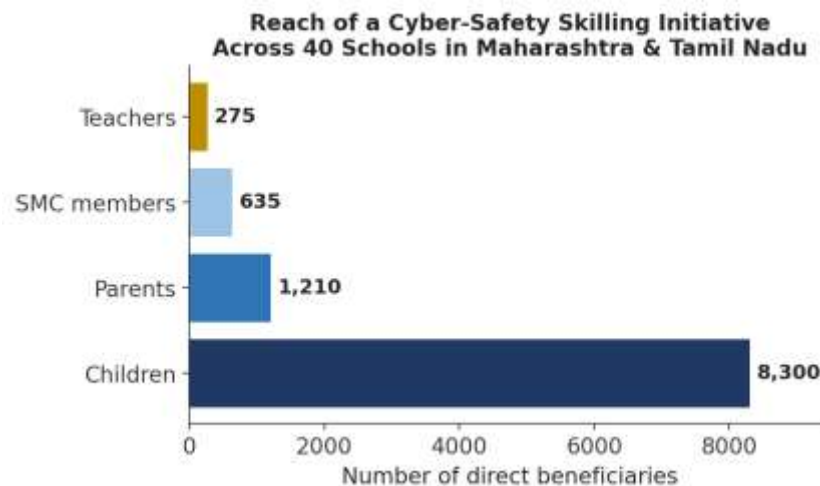
7.5 Evidence That Structured Intervention Works

Figure 12. Change in Cyber-Safety Knowledge Following a Structured School Programme (Index, Baseline = 100)



A structured, in-school cyber-safety skilling programme produced an 81 percent increase in participants' cyber safety knowledge relative to baseline (Gen/Norton et al., 2024) [3]. This is the clearest evidence in the reviewed literature that the awareness gap is tractable: it is not that students are unable to absorb cyber safety concepts, but that structured, dedicated instruction is not yet reaching them at scale.

Figure 13. Reach of a Cyber-Safety Skilling Initiative across 40 Schools in Maharashtra and Tamil Nadu



The same programme reached 8,300 children directly but only 1,210 parents, 635 School Management Committee members and 275 teachers [3] — a ratio that is heavily weighted towards direct student instruction and comparatively light on the adult stakeholders (teachers, parents, institutional bodies) who sustain safe digital habits between formal sessions.

8. Key Findings

- Portal-level cybercrime complaints in India grew approximately 24 percent year-on-year (2024→2025); officially registered cybercrime cases (NCRB) grew 17.9 percent (2023→2024) and crossed 1 lakh for the first time, even as overall registered crime fell 6 percent — cybercrime is now moving in the opposite direction from crime generally [6, 7].
- Fraud accounts for approximately 73 percent of all registered cybercrime motives nationally (2024), far outweighing sexual exploitation, extortion and other motives combined [7].
- Child cybercrime cases rose nearly eightfold between 2018 and 2022 (232→1,823); the NCRB's newer, narrower 2024 measure recorded 1,238 cases, of which 89 percent involved sexually explicit content — closely matching the 64 percent CSAM share found in the fuller 2022 breakdown [7].
- In Haryana specifically, police-led cyber-awareness programmes grew approximately 84 percent and citizen participation grew approximately 46 percent in just four months (Jan–Apr 2025); by mid-2026, Haryana's cyber-fraud recovery rate (31 percent) was running more than eight times the national average (3.85 percent), alongside 3,947 cybercriminal arrests in 2026 alone [2, 10].
- Despite this institutional momentum, independent academic surveys of Haryana higher-education students (n = 500) found overall cybercrime awareness only in the 'average' category, with professional-course students notably more aware than traditional-course students — a gap that state-level enforcement activity alone does not close [1].

- Roughly 7 out of 10 victims of cybercrime did not report the incident, pointing to a parallel gap in response and recourse, not just prevention [4].

9. Proposed Framework: The A-B-I Model

Building on the gaps identified above and the patterns quantified in Section 7, this paper proposes a three-pillar framework for embedding cyber safety and digital wellbeing into student life, referred to here as the A-B-I Model: Awareness, Behaviour and Institutional Support.

9.1 Awareness

The awareness pillar addresses the knowledge gap directly, through age-differentiated curriculum content covering identity and privacy protection, recognition of phishing and social-engineering attempts, safe social media practices, and an understanding of how personal data is collected, stored and monetised online. Content should be differentiated by age band and course stream, given evidence that younger students and traditional-course (non-professional) students show measurably lower awareness than older or professional-course students (Sections 3 and 7.3) [1, 8, 9].

9.2 Behaviour

The behaviour pillar shifts the focus from knowing to doing. This includes practical habit-building around password hygiene, device security settings, verification of sources before sharing information (media literacy), and mindful screen-time management as a component of digital wellbeing rather than of cyber safety alone. Simulated exercises — such as identifying mock phishing messages or auditing one's own privacy settings — can help convert awareness into durable behaviour, and should explicitly include reporting-pathway training given the low reporting rate observed [4].

9.3 Institutional Support

The institutional pillar recognises that individual awareness and behaviour change are insufficient without structural backing: teacher training and capacity-building, clear school-level reporting and response protocols for cyber incidents, partnerships between educational institutions and cyber-safety organisations, and periodic, longitudinal assessment of student awareness and behaviour rather than one-off surveys. At Haryana and national level, current enforcement and outreach efforts are scaling up, and current programmes reach far more students than teachers or parents [2, 3, 10]; correcting this imbalance is what allows gains from the first two pillars to be sustained and scaled beyond individual states, schools or short-term programmes.

The three pillars are designed to operate together rather than sequentially: awareness content is most effective when it is immediately reinforced through behavioural practice, and behavioural change is most likely to persist when it is supported by institutional structures such as teacher involvement and incident-reporting mechanisms.

10. Conclusion and Future Scope

The rapid expansion of digital access among Indian students has not been matched by a corresponding expansion of cyber safety competence, digital wellbeing practices or media literacy. Drawing on recent survey research, the NCRB's official 'Crime in India 2024' report (released May 2026) and Haryana enforcement data current through June 2026, this paper has shown quantitatively that cybercrime volume and its impact on young users are both rising, that awareness gaps are widespread and vary meaningfully by age and institutional stream, and that reporting behaviour lags even further behind preventive awareness [1, 2, 4, 7, 8, 9, 10]. At the same time, evidence from structured interventions — and from Haryana's own

sustained enforcement scale-up — shows that these gaps are tractable when addressed directly. The proposed Awareness–Behaviour–Institutional Support framework offers a structured, scalable starting point for schools, colleges and policymakers seeking to close this gap in a systematic rather than an ad hoc manner.

Future research should move beyond one-time awareness surveys towards longitudinal studies that track whether awareness gains translate into sustained behavioural change and improved reporting rates, and should examine the comparative effectiveness of different delivery models — curriculum-embedded versus workshop-based, teacher-led versus external-partner-led — across India's diverse regional and socioeconomic contexts. Empirical evaluation of a piloted A-B-I framework in a representative sample of Indian schools, with pre/post measurement of the indicators quantified in this paper, would be a natural next step for this line of work.

References

1. M. Choudhary, “Cybercrime Awareness among Higher Education Students from Haryana with Respect to Various Demographical Variables”, *Pal Arch's Journal of Archaeology of Egypt/Egyptology*, 2020, 17 (7), 14454-14461.
2. ETV Bharat, “Cyber Fraud Refund Recovery: Haryana Leads Nation with 31% Success Rate; over 3,900 Cybercriminals Arrested”, July 2026. <https://www.etvbharat.com/en/state/cyber-fraud-refund-recovery-haryana-leads-nation-with-31-percent-success-rate-over-3900-cybercriminals-arrested-enn26070703229>.
3. Gen, Norton, Bal Raksha Bharat (Save the Children India), “Strengthening Cyber Safety Skills for Children in India: Programme Impact Report (March 2023-April 2024)”, 2024.
4. Hamsaveni G., “Awareness of Cybercrime among College Students: A Non-Doctrinal Study”, *International Journal of Scientific Development and Research*, August 2025, 10 (8), b515-b526. <https://ijsdr.org/papers/IJSDR2508163.pdf>.
5. T. Malhotra, M. Malhotra, “Cyber Crime Awareness among Teacher Trainees”, *Scholarly Research Journal for Interdisciplinary Studies*, 2017, 4 (31), 5249-5259.
6. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), “National Cybercrime Statistics 2024-2025”, data reported in industry and policy media, 2025-2026.
7. National Crime Records Bureau (NCRB), Government of India, “Crime in India 2024”, official annual crime report, May 2026.
8. H. Panjani, A. Mudgal, “A Study of Cyber Safety Awareness among Students and Educational Initiatives”, *Indian Journal of Educational Technology*, 2025, 7 (2), 246-256.
9. R. Sahu, K. Rao, Y. Mahalik, “Cybercrime Awareness among Undergraduate Students of Western Odisha: A Survey on Gender and Locality Based Differences”, *RESEARCH REVIEW International Journal of Multidisciplinary*, May 2026, 11 (5), 108-118. <https://doi.org/10.31305/rrijm.2026.v11.n05.011>.
10. Yes Punjab News, “Haryana Cyber Police's National Model: Fraud Halved, Recovery Five Times Higher”, May 2025. <https://yespunjab.com/haryana-cyber-polices-national-model-fraud-halved-recovery-five-times-higher/>.
11. National Council of Educational Research and Training (NCERT), Central Institute of Educational Technology (CIET), “A Study on the Awareness of Cyber Safety and Security among Students”, research report, March 2024.

https://ciet.ncert.gov.in/storage/app/public/files/19/Reportpdf/Research_Cyber%20Safety_Students.pdf