International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Cybersecurity Awareness Among Secondary School Students

Sonali De[1], Ramakanta Mohalik[2], Susmita Priyadarshini[3]

[1]*Student,* [2]*Professor,* [3]*Research Scholar, Regional Institute of Education, NCERT, Bhubaneswar, India*

Abstract- **Cybersecurity awareness is knowledge and understanding of cyber threats, safe online practices, and preventive digital behavior aimed at protecting personal and institutional data. It is especially crucial for adolescent students (generally defined as 10 to 19 years old) because they are at a behaviorally, psychologically, and emotionally formative stage, marked by high digital engagement and limited awareness of online risks. This study aimed to assess the level of cybersecurity awareness among adolescent students and compare it across key demographic factors, including gender, school management type (Government or Private), and board of affiliation (CBSE or State Board). Data was collected using a self-made structured Cybersecurity Awareness Test, which was administered to students aged 15–16 years from eight urban secondary schools in the Bhubaneswar Municipal Commission, Odisha, India. The sample included 297 students: 185 from government schools and 112 from private schools, of which 177 were from Central Board of Secondary Education (CBSE) affiliated schools and 120 from State Board-affiliated schools. Descriptive and inferential statistics revealed that while overall awareness was moderate (M = 12.0 out of 21), significant differences were found based on Board of affiliation and School type. CBSE-affiliated and private school students demonstrated higher awareness than their State Board and government school.The study has implications for curriculum designers, and school administrators, emphasizing the urgent need for integrating structured and inclusive cybersecurity education in schools, particularly for the underperforming groups, in a targeted manner.**

Keywords- **Cybersecurity Awareness, Adolescents, Bhubaneswar, Curriculum, Gender.**

I. INTRODUCTION

With the increasing integration of technology into everyday life, individuals are more exposed to cyberspace than ever before. This shift has been accelerated by post-COVID digitization of Education. Integration of technology has been strongly emphasized in India’s National Education Policy (NEP) 2020 and the National Curriculum Framework for School Education (NCFSE) 2023, which advocate for digital learning, blended classrooms, and the ethical use of technology (Ministry of Education, 2020; 2023). As digital infrastructure expands, so too does the risk landscape.

Research shows a rapid increase in the frequency, scale, and sophistication of cybercrimes globally and especially in India. AI-powered threats and targeted attacks on educational institutions has increased as well (Chambers, 2025; SOCRadar, 2024; India Today, 2024).

In this evolving context, cybersecurity awareness has become a critical life skill. Studies have consistently highlighted that awareness levels remain moderate at best, with significant gaps in understanding advanced threats, safe practices, and legal mechanisms (Kumar & Singh, 2018; Sharma, 2019; Hasan et al., 2025). Awareness also varies by demographic factors. For example, Verma& Kushwaha (2021) found boys had higher awareness than girls, while private school students scored better than government school peers. Joshi & Desai (2017) observed urban-rural disparities, while Titi (2025) and Florendo et al. (2025) reported awareness increasing with academic level and discipline.

Cybersecurity awareness is defined as the knowledge and understanding of cyber threats, safe online practices, and the fundamental importance of protecting digital assets (NIST, 2024; Government of India, 2013; National Cyber Security Policy, 2013). To standardize this concept, particularly in the context of adolescents, this research adopts "A Handbook for Adolescents/Students on Cyber Safety" by the Ministry of Home Affairs (2021) as its key reference. Based on this foundational document, cybersecurity awareness is conceptualized as encompassing an understanding of potential digital threats (e.g., phishing, malware, identity theft), an awareness of safe online practices (such as utilizing strong passwords, activating privacy settings, and avoiding suspicious links), and a grasp of preventive strategies and appropriate reporting mechanisms. Specifically, the study measures awareness through a self-made structured test across three core dimensions: Threat Identification (knowledge about cyberbullying, cyber grooming, financial fraud, and identity theft), Awareness of Risks and their Mitigation (understanding safe online practices and tools for malware detection), and Safe Digital Practices (promoting responsible technology use and critical evaluation of online content).

Globally, research indicates that while basic awareness of cyber threats exists among students, it is often superficial and does not translate into protective behavior. For instance, Abdullahi (2023) and Zulkifli et al. (2020) reported moderate conceptual awareness but poor application among high school students. In India, this pattern is echoed in the works of Kumar & Singh (2018) and Patel & Mehta (2020), who noted a worrying gap between theoretical knowledge and real-world digital safety practices. International comparisons further highlight that it varies widely across demographic groups and educational contexts. Studies by Verma& Kushwaha (2021) revealed significant disparities based on gender and school type, while Joshi & Desai (2017) underscored the urban-rural digital divide.

Despite a growing body of work, adolescents—a particularly vulnerable group due to their high digital exposure and psychological susceptibility—remain underrepresented in research. This gap is especially pronounced in the Indian context, where only a few empirical studies have specifically targeted this age group. Moreover, regional research on cybersecurity awareness is limited. Odisha, despite its advancing digital infrastructure under initiatives like the Bhubaneswar Smart City mission, has received scant scholarly attention regarding school-level cybersecurity. No comparative study has yet examined the influence of school type or board affiliation on adolescents in this region. Several key factors: NEP 2020's emphasis on the critical role of technology in improving access, equity, and quality in education and its call for ensuring digital safety, particularly in school environments; The rapid digitalization of education, especially post-pandemic, which has led to students facing increased exposure to cyber risks and; Significant research gaps in understanding cybersecurity awareness among adolescents, particularly in regional contexts like Odisha thus forms the rationale for this study. Bhubaneswar, therefore, presents an ideal setting for this study.

The findings of this study provide valuable insights for educational policymakers, curriculum developers, and school administrators aiming to enhance cybersecurity preparedness among secondary school students. By identifying variables that significantly affect awareness levels, it offers evidence-based recommendations for targeted interventions. These findings underscore the role of curriculum design, access to technology, and institutions in shaping student awareness.

Strengthening digital safety education, particularly within the State Board framework, is necessary to equip all students with the knowledge and skills necessary to navigate the digital world safely and responsibly. Thus, the broader goal of equity and inclusion in digital education as envisioned in NEP 2020 can be realized.

II. Objectives

1. To describe the level of cybersecurity awareness among secondary school students.
2. To compare the cybersecurity awareness of secondary school students based on gender.
3. To compare the cybersecurity awareness of secondary school students based on type of school (Government and Private).
4. To compare the cybersecurity awareness of secondary school students based on educational board (CBSE and State Board).

III. Hypotheses

For the objectives numbered 2, 3 and 4 the following null hypotheses were formulated.

($H_0$1): There is no significant difference in cybersecurity awareness between male and female secondary school students.

($H_0$2): There is no significant difference in cybersecurity awareness between students from government and private secondary schools.

($H_0$3): There is no significant difference in cybersecurity awareness between students studying in CBSE and State Board schools.

IV. Method

The present study employed quantitative design followed by survey method, for assessing the level of cybersecurity awareness among secondary school students and comparing it across the selected demographic variables. The population consisted of students enrolled in classes 9 and 10 from eight urban secondary schools within the Bhubaneswar Municipal Corporation (BMC) area, Odisha, India. Stratified Random Sampling technique was adopted to ensure balanced representation while selecting the sample across two key strata: School Management type (government vs. private) and educational board of affiliation (CBSE vs. State Board).

The final sample consisted of 297 students (163 male and 134 female), comprising 185 from government schools and 112 from private schools. Board-wise, 177 students were affiliated with Central Board of Secondary Education (CBSE) and 120 with the State Board (BSE).

To measure cybersecurity awareness, a self-developed structured test was administered, owing to the absence of relevant recent standardized tools contextualized for secondary students. The test items were derived from the *Handbook for Adolescents/Students on Cyber Safety* (Ministry of Home Affairs,Govt. of India, 2021) to ensuring alignment with the national policies and curricular relevance. Three dimensions were taken into consideration while preparing the test items they are- threat identification, awareness of risks and safeguarding data. Initially 44 multiple-choice items were prepared for the tool, that has subsequently refined to 21 items following a pilot test with 20 students and expert review. Items were selected based on clarity, developmental appropriateness, and balance across three dimensions. The Cronbach Alfa reliability is of 0.71, which indicates a high reliability of the test. Hence the content validity of the tool was ensured. The distribution of items across dimensions is summarized in table 1.

Table 1
Dimensions of the cyber security awareness

Dimensions	*No. of Items*
Threat Identification	**7**
Awareness of Risks	**7**
Safeguarding Data	**7**
Total	**21**

Data collection was conducted offline during school hours in the presence of respective subject teachers. Analysis was carried out by using SPSS, employing descriptive statistics and independent samples t-tests at 0.05 levels.

V. Data Analysis And Interpretation

The data were analyzed using both descriptive and inferential statistical techniques, as per the study's objectives.

For the first objectives, the investigator categorized the level of cybersecurity awareness of students on the basis of the scores obtained and using the Normal Probability Curve. The study reveals that majority of students (69.7%) are “Aware” indicating the foundations of digital security concepts are apprehended properly, while 15.5% are “Well Aware,” showing a critical grasp and 14.8% were classified as “Less Aware’ suggesting that few students are struggling to recognize the potential threats and may not know how to responds to cyber threats. The group-wise categorization is indicated in table 2.

Table 2
Level of cyber security awareness of secondary school students

		Less Aware	***Aware***	***Well Aware***	***Number of Students***
Overall Distribution	Overall	44 (14.81%)	207 (69.70%)	46 (15.49%)	297
Gender	Male	26 (15.95%)	118 (72.39%)	19 (11.66%)	163
	Female	18 (13.43%)	89 (66.42%)	27 (20.15%)	134
School Type	Government	37 (20.00%)	119 (64.32%)	29 (15.68%)	185
	Private	7 (6.25%)	88 (78.57%)	17 (15.18%)	112
Board of Affiliation	CBSE	15 (8.48%)	119 (67.23%)	43 (24.29%)	177
	State Board	29 (24.17%)	88 (73.33%)	3 (2.50%)	120

**Based on the total scores of the 297 participants and applying the Normal Probability Curve. < 7.89 (Less Aware); 7.89 – 16.04 (Aware); > 16.04 (Well Aware)*

As evident from table 2 and Figure 1, the gender-wise distribution of cybersecurity awareness indicates important patterns in students’ knowledge levels.

The data reveals that majority of both male and female students fall within the 'Aware' category with 66.42% of females and 72.39% of males demonstrating a moderate level of awareness, this suggests most of the students irrespective of their genders shows possesses a foundational understanding of cybersecurity concepts.

Interestingly, a more detailed investigations reveals more females (20.15%) than males (11.66%) fall into the 'Well Aware' category, suggesting higher awareness among female students, suggests that while both the genders shows basic cybersecurity awareness, female students tend to exhibit advanced cybersecurity knowledge.

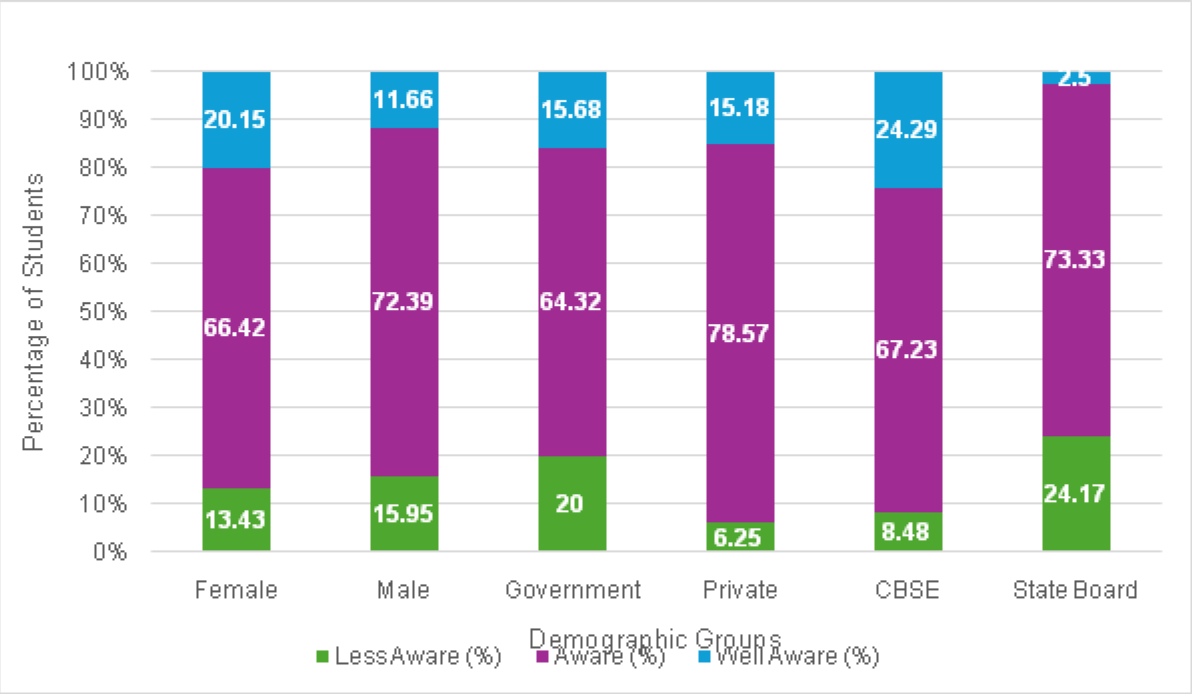

Figure 1 Level of cybersecurity awareness across demographic groups

On analyzing cyber security awareness across different schools' type, a relevant pattern has been recognized. While government school students showed a higher count with 64.32% across all awareness levels, private school students exhibited notably stronger cybersecurity awareness. Only 6.25% of private schools fell into 'Less Aware' category while a higher proportion of government schools' students with 20 % of in total comes under the same category indicating relatively better cybersecurity awareness among the private school students. Interestingly, both school types showed comparable proportions in 'well-aware' category with 15.18 for private schools and 15.68 for government schools, indicating both the schools produces equivalent numbers of highly aware cybersecurity students.

The comparison of schools based on board affiliation revels more pronounced disparities. CBSE students exhibit significantly higher awareness, with 24.29% falling under the 'Well Aware' category as opposed to only 2.50% from the State Board, this demonstrates the striking gap underscores significant inequalities in cybersecurity awareness across the curricula. Additionally, a higher proportions of state board students (24.29%) falling under less aware category as compared to CBSE students (8.48%). This indicates there lies a critical gap among CBSE and state board schools in cybersecurity awareness.

Table 3
Descriptive analysis of Cybersecurity Awareness scores (Gender-wise)

Statistic	*N*	*Mean*	*SD*	*Mean Diff.*	*Mann-Whitney U value*	*p-value*
Male (M=1)	163	11.6	4.14	-1.000	9553	0.160
Female (F=2)	134	12.4	3.98			

The investigator has conducted a comprehended comparison on cybersecurity awareness scores among male and female students by using descriptive and inferential statistics. For the inferential statistical analysis, the group means of male and female students were compared using the Mann-Whitney *U* test, which is a non-parametric statistical test (as the scores were not normally distributed) for comparing group means. The mean scores of the male and female groups of students in cybersecurity awareness were compared against the null hypothesis of H_0 : µ_male = µ_female, i.e., no significant difference between the group means of the cybersecurity awareness score with respect to gender. The significance level was fixed as $\alpha = 0.05$. The statistical figures for the Mann-Whitney test, along with the respective p-values, have been reported in Table 3. These results suggest that gender plays a vital role in cybersecurity awareness among secondary school students.

FurtherIt is found that the Mann-Whitney *U* test result is $U = 9553$ and a p-value of 0.160. Since $p = 0.160 > \alpha = 0.05$, the null hypothesis could not be rejected at the 0.05 level of significance. It can be concluded that there is no significant difference between the cybersecurity awareness of students at the secondary level with respect to gender (U = 9553, $p = 0.160 > \alpha = 0.05$). Thus, there is no statistically significant difference among the scores of the male and female groups of students with respect to overall cybersecurity awareness.

Table 4
Comparison between groups (by School type)

School Type	*N*	*Mean*	*SD*	*Mean Diff.*	*Mann-Whitney U value*	*p-value*
Government	185	11.6	4.36	-1.000	9140	0.088
Private	112	12.5	3.49			

The descriptive statistical analysis of total scores for government and private school students is indicated in Table 4. The mean cybersecurity awareness score for the government school group is 11.6, while it is 12.5 for the private school group. The standard deviation about the mean was also calculated for both the groups, and it was found that the government school group showed a standard deviation of 4.36 while that of the private school group standard deviation is 3.49.

For the inferential statistical analysis, the group means of government and private school students were compared using the Mann-Whitney *U* test, which is a non-parametric (as the scores were not normally distributed) statistical test for comparing the group means. The mean scores of the government and private groups of students in cybersecurity awareness were compared against the Null hypothesis of H_0=µGovernment =µPrivate, i.e., no significant difference in the group means of the cybersecurity awareness score with respect to school type. The test was done using Jamovi and at the significance level of α=0.05. The statistical figures for the Mann-Whitney test, along with the respective P values, have been reported in Table 4.

It is found that the Mann-Whitney *U* test results are U=9140 and P value of P=0.088. P=0.088 >α=0.05, hence the null hypothesis is not rejected at the 0.05 level of significance. It can be concluded that there is no significant difference between the cybersecurity awareness scores of students at the secondary level with respect to school type (U=9140, P=0.088 >α=0.05).

Table 5
Comparison between groups (by Educational Board)

Education Board	*N*	*Mean*	*SD*	*Mean Diff.*	*Mann-Whitney U value*	*p-value*
CBSE	177	13.7	3.77	5.00	4036	< .001*[i]
BSE	120	9.45	3.11			

Table 5 indicates the descriptive statistical analysis of total scores for CBSE and BSE board students. The mean cybersecurity awareness score for the CBSE group is 13.7 while it is 9.45 for the BSE group. The standard deviation about the mean was also calculated for both the groups, and it was found that the CBSE group showed a standard deviation of 3.77, while that of the BSE group standard deviation is 3.11. The minimum total score for the CBSE group was 2, while it was found to be 2 for the BSE group. The maximum cybersecurity awareness score for the CBSE and BSE groups was 21 and 17, respectively. For the inferential statistical analysis, the group means of CBSE and BSE students were compared using the Mann-Whitney *U* test. The mean scores of the CBSE and BSE groups of students in cybersecurity awareness were compared against the Null hypothesis of H_0= μCBSE =μBSE, i.e., no significant difference in the group means of the cybersecurity awareness score with respect to educational board. The test was done using JAMOVI and at the significance level of α=0.05. The statistical figures for the Mann-Whitney *U* test, along with the respective P values, have been reported in Table 5.

It is found that the Mann-Whitney *U* test results are *U*=4036 and *P* value of *P*=<.001. *P*=< .001 <α=0.05, hence the null hypothesis is rejected at the 0.05 level of significance. It can be concluded that there is a statistically significant difference between the cybersecurity awareness scores of students with respect to the educational board (*U*=4036, *P*=< .001 <α=0.05) with CBSE group scoring significantly higher than the BSE group of students with respect to overall cybersecurity awareness.

For instance, Private CBSE students demonstrated the largest highly statistically significant difference in awareness when compared to Government State Board students (Mean Difference = 5.09, *p*< .001). A statistically significant difference was also identified between Government State Board and Private State Board students (Mean Difference = -1.80, *p* = 0.009), suggesting that private State Board students have significantly higher cybersecurity awareness than their government counterparts within the State Board system. These findings underscore the influence of curriculum design over school management type in determining cybersecurity awareness.

VI. Major Findings

- The study examined the level of awareness among 297 secondary school students, the findings revealed a moderate level of cybersecurity awareness with a mean score of 12.0 out of 21. Further analysis shows a tripartite distribution where 14.81% were classified as 'Less Aware', while a significant majority (69.70%) possessed a moderate level and classified as 'Aware', and 15.49% demonstrated high awareness and classified under 'Well Aware'. The result suggests while a basic understanding and awareness exists among most of the students, there is a need for interventions that will allow them to improve their understandings.
- Analyzing the influencing factors revealed that gender was not a significant determinant of cybersecurity awareness as there is no significant difference between the cybersecurity awareness of students at the secondary level with respect to gender (U = 9553, *p* = 0.160 > α = 0.05). This implies the null hypothesis could not be rejected at the 0.05 level of significance, suggesting that cybersecurity awareness among secondary school students is independent of gender.
- Similarly, the school type that is government and private, did not appear to be a significant factor that influence cybersecurity awareness as the result showed no significant difference in awareness scores of students at the secondary level with respect to school type (Government vs. Private) (*U*=9140, *P*=0.088 >α=0.05) leading to the acceptance of null hypothesis at 0.05 level of significance. However, post-hoc tests of school type within the school board revealed a notable exception with private school students showing significantly better awareness than their government school counterparts.

- In contrast, the students educational board emerged to be a primary significant factor with statistically high significant difference (*U*=4036, *P*=< .001 <α=0.05) on cyber-security awareness among the respective groups i.e. CBSE and State board. Where CBSE board students scores significantly higher than that of the state board students (BSE Students). This is further supported by the post-hoc tests which revealed that both Government CBSE and Private CBSE students had significantly higher awareness than both Government and Private State Board students. This disparity was consistent across the different school types, with both Govt. and Private CBSE Students exhibits markedly higher awareness score than both Govt. and Private State Board students.
- The study concludes that the educational board is considered to be the primary determinant of cybersecurity awareness, with CBSE students being significantly more aware. The notably lower awareness among State Board students, particularly in government schools, indicates a need for targeted educational interventions to improve their cybersecurity knowledge.

VII. Discussion

The study explored the level of awareness among secondary school students with respect to the influence of demographic variables i.e., gender and institutional variables i.e, school types (government and private) and boards (CBSE and State board). The results provide an insightful information on the participants awareness on Cyber security and their potential effect across the dimensions.

The findings revealed a moderate level of overall cybersecurity awareness among secondary school students, with a mean score of 12.0 out of 21. Among the 297 participants, 14.81% were classified as 'Less Aware', 69.70% as 'Aware', and 15.49% as 'Well Aware'. This observation corroborates similar research on adolescent cybersecurity knowledge. For instance, studies by Dapitan et al. (2024) and Taso et al. (2023) also reported that while students often grasp basic cyber threats, they frequently lack an in-depth understanding of practical online safety measures. Furthermore, consistent with Al Shabibi and Al-Suqri (2023), increased digital exposure in this cohort did not necessarily translate into improved practical cybersecurity behaviors, a theory-practice gap also highlighted in Indian contexts by Kumar and Singh (2018) and Patel and Mehta (2020).

The analysis of gender difference indicated that Gender was not a significant determinant of cybersecurity awareness although females exhibited slightly higher awareness levels, with 20.15% being 'Well Aware' compared to 11.66% of males, this difference is not statistically significant. Among males, a larger proportion (15.95%) fell under the 'Less Aware' category compared to females (13.43%). While females exhibited a marginally higher mean score, this difference was not significant. This outcome contrasts with findings from Verma and Kushwaha (2021), which previously reported higher awareness among male students. However, this outcome aligns with Elfadil (2021) and Alrobaian et al. (2023), suggesting a potential narrowing of the digital gender divide in digitally saturated urban environments like Bhubaneswar, thus indicating a shift in gender-based digital literacy dynamics.

With respect to the types of schools, the study found no statistically significant difference in cybersecurity awareness between government and private school students. Private school students showed somewhat better awareness, with 15.18% classified as 'Well Aware', as against 15.68% in government schools, and a much lower percentage of 'Less Aware' students (6.25% in private vs. 20.00% in government schools). This finding partially supports Joshi and Desai (2017), who observed negligible differences in urban areas with uniform digital infrastructure, and could reflect the positive influence of broader initiatives such as the Smart City Mission in Bhubaneswar. This diverges from other research, like that of Verma and Kushwaha (2021), which attributed higher awareness to private schools due to more advanced digital curricula. The present study suggests that when infrastructure and exposure are comparable, school management type alone may not be a decisive factor in digital literacy outcomes.

When analyzed by board affiliation, CBSE-affiliated students demonstrated noticeably higher awareness, with 24.29% being 'Well Aware' and only 8.48% falling under the 'Less Aware' category. In contrast, State Board students had the lowest proportion of 'Well Aware' (2.50%) and the highest share of 'Less Aware' (24.17%). These findings suggest a disparity in awareness aligned with board affiliation, warranting further investigation. Crucially, the educational board emerged as a highly significant determinant of cybersecurity awareness. CBSE students demonstrated markedly higher awareness (mean 13.7) compared to their State Board counterparts (mean 9.45), indicating a substantial and statistically significant difference.

This strongly suggests that the educational board plays a pivotal role in shaping students' cybersecurity knowledge. This finding is consistent with arguments made by Sharma (2019) and Dasgupta and Chatterjee (2020), who highlighted curricular disparities and a more thorough integration of ICT and cybersecurity content within CBSE schools. Further analysis reinforced this, showing that CBSE students, irrespective of school type, consistently outperformed State Board students. Additionally, within the State Board system, private school students exhibited significantly greater awareness than government school students, hinting at the influence of resource availability and school-level initiatives, as noted by Bhatia (2020). These results underscore the profound impact of curriculum design and institutional policies (Reddy and Rao, 2019), emphasizing the need for systemic reforms in curriculum and teacher training, particularly within State Board schools (Garg et al., 2021), to bridge the observed digital literacy gap.

VIII. Conclusion

This study on cybersecurity awareness among adolescent students in Bhubaneswar reveals an overall moderate level of understanding regarding cyber threats, safe online practices, and digital hygiene. Crucially, the research identified significant disparities in awareness, primarily driven by educational board affiliation, with CBSE-affiliated students demonstrating notably higher levels of awareness compared to their State Board counterparts. This profound influence of the educational board strongly suggests that curriculum content and structure play a pivotal role in shaping students' cybersecurity literacy. In contrast, gender differences in cybersecurity awareness were minimal and not statistically significant, indicating a potential narrowing of the digital gender divide in urban settings like Bhubaneswar. Similarly, no statistically significant difference was found between government and private school students, which may reflect the impact of comparable digital infrastructure and exposure in urban environments. These findings underscore that, in this context, factors beyond gender or school management type are the primary determinants of digital literacy outcomes.

The study contributes localized, empirical data from a rapidly digitizing urban center, enriching the discourse on digital literacy and student safety in India. It holds practical implications for educational policymakers, curriculum designers, and school administrators, emphasizing the urgent need for targeted, evidence-based interventions. Strengthening digital safety education, particularly within the State Board framework, is essential to equip all students with the skills to navigate the online world safely. By addressing these disparities and focusing on comprehensive curriculum reforms, the broader goals of digital equity and inclusion, as envisioned by India’s National Education Policy (NEP) 2020 and the National Curriculum Framework for School Education (NCFSE) 2023, can be progressively achieved. While this cross-sectional study provides a snapshot of awareness, future longitudinal research in diverse geographic regions could offer deeper insights into the evolving landscape of cybersecurity literacy.

REFERENCES

[1] Abdullahi, M. (2023). Cyber safety perceptions among African high school students. Journal of Digital Youth Studies, 9(2), 87–102.

[2] Alrobaian, L., Alshamrani, A., &Alharthi, H. (2023). Gender and cybersecurity: Awareness and practices among adolescents in Saudi Arabia. Cyberpsychology Reports, 5(1), 33–45.

[3] Al Shabibi, A. S., & Al-Suqri, M. N. (2023). Youth digital behaviors and cybersecurity awareness in Oman. Middle East Journal of Information Security, 14(2), 56–72.

[4] Bhatia, K. (2020). Digital education in Indian schools: Equity and access issues. New Delhi: Centre for Educational Development.

[5] Chambers, J. (2025). The evolving threat landscape: Implications for educational institutions. Global Journal of Cybersecurity, 12(1), 45–60.

[6] Dasgupta, S., & Chatterjee, R. (2020). ICT integration and curriculum reforms in CBSE and State Boards: A comparative analysis. Indian Journal of Education Policy, 6(3), 14–27.

[7] Dapitan, R. M., Soriano, F. J., &Laborte, A. P. (2024). Evaluating senior high school students’ cyber hygiene in the Philippines. Asia-Pacific Journal of Educational Technology, 11(2), 102–114.

[8] Elfadil, A. E. (2021). Gender differences in cybersecurity awareness among Sudanese adolescents. African Journal of Cyber Education, 3(1), 59–70.

[9] Florendo, R. A., Hernandez, M. J., &Teves, C. (2025). Disciplinary variation in digital security knowledge among college entrants. International Journal of Digital Pedagogy, 8(1), 23–39.

[10] Garg, A., Sinha, M., &Mehra, P. (2021). Teacher preparedness and cybersecurity education in India. Contemporary Educational Research Journal, 4(2), 91–103.

[11] Gen Digital. (2025). Digital lives of Indian teens: A trend report. Gen Digital Research Division. https://www.gendigital.com

[12] Hasan, Z., Mukherjee, S., & Khan, R. (2025). Adolescent vulnerability to online scams: A behavioral study. Indian Journal of Cybersecurity Research, 7(1), 18–31.

[13] India Today. (2024, March 12). Rise in student-targeted phishing and malware attacks in India. https://www.indiatoday.in/tech

[14] Joshi, V., & Desai, R. (2017). Urban-rural differences in internet safety practices of Indian teenagers. Journal of Adolescent Digital Behavior, 5(3), 78–91.

[15] Kumar, A., & Singh, R. (2018). Cybersecurity knowledge among high school students in India: Gaps and implications. Indian Journal of Educational Technology, 13(1), 32–40.

[16] Ministry of Education. (2020). National Education Policy 2020. Government of India. https://www.education.gov.in

[17] Ministry of Education. (2023). National Curriculum Framework for School Education (NCFSE). Government of India. https://ncf.ncert.gov.in

[18] Ministry of Home Affairs. (2021). A handbook for adolescents/students on cyber safety. Government of India. https://cybercrime.gov.in

[19] Patel, S., & Mehta, D. (2020). Online safety practices among Indian secondary school students. South Asian Journal of Education, 9(2), 102–116.

[20] Reddy, S. C., & Rao, D. N. (2019). Institutional policy and its role in promoting digital citizenship. Indian Journal of School Leadership, 7(4), 120–134.

[21] Shaikh, N., Kapoor, P., & Dutta, B. (2021). Adolescents in the digital age: Cyber safety challenges in India. Journal of Indian Child Psychology, 4(2), 45–62.

[22] Sharma, R. (2019). ICT awareness and cybersecurity education in Indian curriculum. Journal of Educational Research and Innovation, 6(1), 55–66.

[23] SOCRadar. (2024). India Threat Landscape 2024. SOCRadar Cyber Intelligence. https://socradar.io

[24] Taso, M. A., Rojas, A. C., & Medina, L. R. (2023). High school students' cybersecurity skills in Peru. Latin American Journal of Digital Literacy, 3(2), 75–84.

[25] Titi, M. (2025). Cyber awareness progression across academic levels in secondary education. Middle East Cyber Education Review, 6(1), 15–27.

[26] Verma, S., & Kushwaha, N. (2021). Gender and institutional influences on digital safety awareness. Journal of Cyber Psychology and Schooling, 10(3), 88–98.

[27] Zulkifli, N. A., Ismail, Z., & Nor, M. (2020). Cybersecurity awareness among Malaysian high school students. International Journal of Cyber Education, 5(2), 101–116.

[i] Statistically significant