

Understanding Cyber Crime Awareness Levels Among School Students: A Quasi-Experimental Study in Dehradun

Raj Vishnoi^{1*}, Sangam Sharma², Kusum Lata³, Diksha Bahuguna⁴

¹ Assistant Professor (Dep. of Child Health Nursing), Doon Institute of Medical Sciences, Dehradun, Orcid Id: <https://orcid.org/0009-0000-9367-6701>

² Assistant Professor (Dep. of Mental Health Nursing), Doon Institute of Medical Sciences, Dehradun.

³ Assistant Professor (Dep. of Medical Surgical Nursing), Doon Institute of Medical Sciences, Dehradun.

⁴ Nursing Tutor (Dep. of Mental Health Nursing), Dev Bhoomi Uttarakhand University.

Abstract

Background: Children and teenagers face growing exposure to severe digital risks, including cyberbullying, privacy intrusions, and financial fraud, the latter of which accounted for 69% of all cybercrime instances in India in 2023. Because young people are highly susceptible to online abuse and digital threats, incorporating age-appropriate cybersecurity education is a vital requirement to close the gap in digital safety.

Methods: A quantitative, one-group pre-test/post-test quasi-experimental study was conducted among school students aged 12 to 18 in Dehradun. Using a demographic interview schedule and a self-structured multiple-choice questionnaire, researchers evaluated a sample of 60 students. Participants completed a baseline pre-test, attended a 45-minute interactive audio-visual awareness session on cybercrime prevention, and completed a post-test on the seventh day to measure knowledge retention.

Results: Baseline assessments indicated a severe lack of digital literacy, with 65.0% of respondents exhibiting inadequate awareness, 31.7% showing moderate awareness, and only 3.3% demonstrating adequate awareness. Following the intervention, awareness levels shifted significantly: inadequate awareness dropped to 6.7%, moderate awareness rose to 71.7%, and adequate awareness climbed dramatically to 21.7%. The intervention yielded a highly significant increase in the mean knowledge score, moving from 13.55 in the pre-test to 20.83 in the post-test ($p < 0.001$). Furthermore, baseline awareness levels showed no statistically significant associations with demographic variables such as age, gender, educational standard, digital exposure, or primary device used.

Conclusion: School students exhibit a severe baseline lack of cybercrime awareness, independent of their demographics or daily digital habits. However, a structured 45-minute audio-visual intervention significantly improved their knowledge, drastically reducing the rate of inadequate awareness from 65% to 6.7%. This demonstrates that formal, school-based cybersecurity education is highly effective and an essential requirement for equipping youth with proactive digital defense mechanisms.

KEYWORDS: Cybercrime, Cybersecurity Education, Digital Literacy, School Students, Quasi-Experimental Study, Digital Safety and Awareness Program.

Introduction

Although children and teenagers are exposed to serious digital risks including cyberbullying, online predators, and privacy intrusions, the internet is an indispensable component of everyday life. As young people have early, unlimited access to cyberspace, cybercrimes—illegal activities performed via digital networks for financial gain, exploitation, or disruption—are fast increasing. Financial fraud accounted for 69% of all cybercrime instances in India, which increased by 31% to 86,420 in 2023. With 1,832 incidents documented in 2022, crimes expressly targeting minors are also on the rise. These crimes are mostly related to cyberpornography, stalking, and bullying.

According to data, 63.8% of kids are exposed to cyber dangers, with 14.9% experiencing cyberbullying and 13.6% considering suicide as a result of pressure from the internet. The Information Technology Act, 2000 and the modified Indian Penal Code penalize transgressions in order to counter these dangers. Local police, the National Cybercrime Reporting Portal, and the 1930 national hotline are all easily accessible reporting channels.

NEED OF THE STUDY - Because of their intense passion for technology and games, young people are more susceptible to online abuse and unintentional participation in harmful activities (such as virus writing). Incorporating age-appropriate cybersecurity education is a vital requirement rather than a choice in a society that is digitizing quickly. By concentrating on important educational goals for teens, this study is necessary to close the gap in digital safety. Teaching young people how to manage their expanding digital footprints, safeguard data privacy, and comprehend the long-term effects of their online behavior on their reputations are some of these goals. Teenagers must also learn how to see warning signals, protect accounts, and properly report cyberbullying in addition to being prepared to notice and steer clear of growing cyberthreats like phishing and financial fraud. Teens may build safe online behaviors and even find future employment prospects in cybersecurity by learning about digital rights and ethics via real-life case studies.

MATERIAL AND METHODS – A quantitative, one-group pre-test/post-test quasi-experimental design. 60 students (aged 12–18) from a selected secondary school in Dehradun, chosen via simple random and systematic sampling. Data was collected using a demographic interview schedule and a self-structured multiple-choice awareness questionnaire. Tool reliability was validated through a pilot study using Cronbach’s alpha. Participants completed a baseline pre-test, followed by a 45-minute interactive audio-visual awareness session on cybercrime prevention. A post-test was administered on the 7th day to measure knowledge retention. Data is analyzed using descriptive statistics (mean, median, standard deviation) to evaluate awareness scores. Inferential statistics, specifically paired t-tests, measure the intervention's effectiveness, while Chi-square tests evaluate associations between baseline knowledge and demographic variables at a 0.05 significance level

RESULTS – Section A: Demographic Characteristics

Table 1: Frequency and percentage distribution of Demographic Characteristics N = 60

Demographic Variable	Category	Frequency	Percentage (%)
Age	10 to 12 years	22	36.7
	13 to 15 years	18	30.0
	16 to 18 years	20	33.3
Gender	Male	26	43.3
	Female	34	56.7
Current Standard	9th - 10th Standard	55	91.7
	11th - 12th Standard	5	8.3
Digital Exposure	1 - 2 Hours	39	65.0
	3 - 5 Hours	19	31.7
	6 - 8 Hours	2	3.3
Primary Device	Mobile phone	41	68.3
	Computer	4	6.7
	Laptop	9	15.0
	Other	6	10.0
Previous Knowledge	Yes	6	10.0
	No	54	90.0

Table 1 presents the demographic profile of the 60 respondents included in the study. - In terms of age distribution, the participants are fairly evenly divided into three categories, the biggest of which is 10 to 12 years old (36.7%), followed by 16 to 18 years old (33.3%) and 13 to 15 years old (30.0%). The gender distribution shows that 56.7% of the sample is female, with the remaining 43.3% being male. Regarding educational background, the vast majority of respondents (91.7%) are presently enrolled in the 9th to 10th standard, while just a little portion (8.3%) are in the 11th to 12th standard. According to the statistics, the majority of participants (65.0%) use digital devices for one to two hours per day. Only 3.3% report spending 6 to 8 hours every day, while almost one-third (31.7%) report 3 to 5 hours.

The mobile phone is the most prevalent primary device, predominantly utilized by 68.3% of the respondents. Alternate primary devices include laptops (15.0%), computers (6.7%), and other unspecified devices (10.0%). Finally, regarding baseline familiarity, a significant majority (90.0%) reported having no previous knowledge of the subject matter, while only 10.0% indicated having prior awareness. Section B: Assessment of pretest and post-test level of knowledge regarding cyber-crime and its prevention among school going children.

Table 2: Frequency and percentage distribution of level of knowledge regarding cyber-crime and its prevention among school going children
N = 60

Level of Awareness	Pre-Test		Post-Test	
	Frequency	Percent	Frequency	Percent
Adequate Awareness	2	3.3%	13	21.7%
Inadequate Awareness	39	65%	4	6.7%
Moderate Awareness	19	31.7%	43	71.7%
Total	60	100%	60	100%

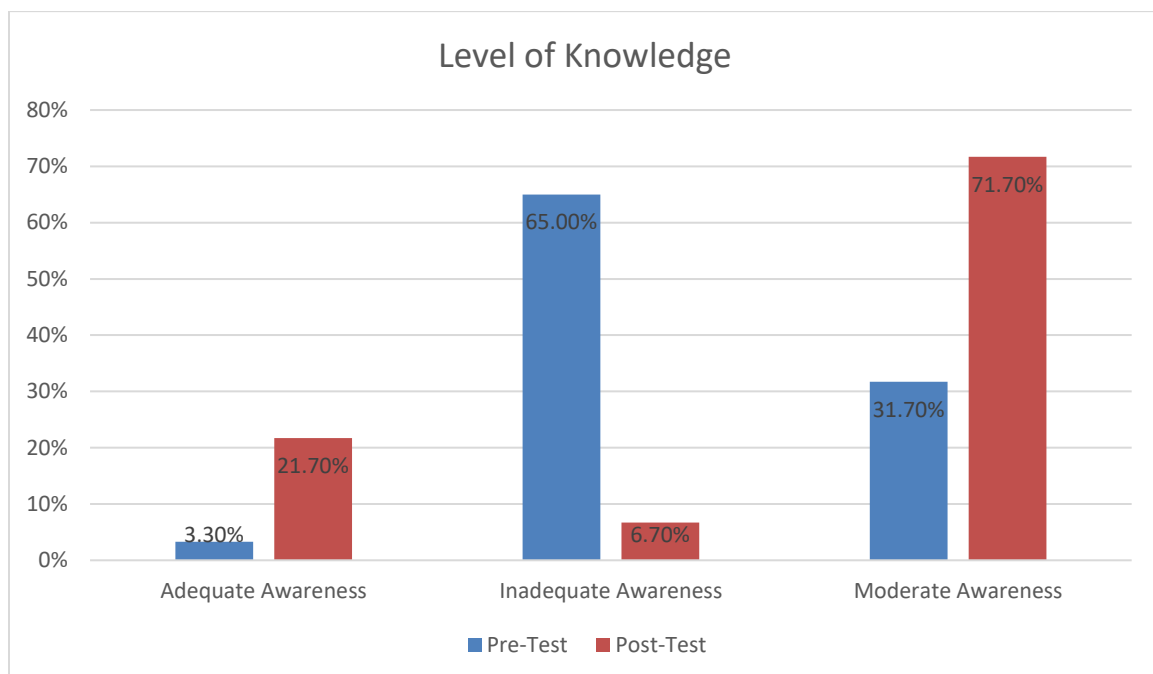


Figure 1: Bar chart showing percentage distribution of knowledge regarding cyber-crime and its prevention among school going children

The respondents' awareness levels before to the intervention are shown in Table 2 and Figure 1. 'Inadequate Awareness' was exhibited by the majority, 65.0% (n=39). Only 3.3% (n=2) of the subjects demonstrated "Adequate Awareness," whereas 31.7% (n=19) had "Moderate Awareness." The majority, 71.7% (n=43), now exhibit "Moderate Awareness," indicating a discernible change. While the percentage of respondents with "Inadequate Awareness" dropped to 6.7% (n=4), the percentage of respondents with "Adequate Awareness" climbed dramatically to 21.7% (n=13).

Section C: Efficacy of awareness program regarding cybercrime and its prevention

Table 3: Paired T Test Showing Effectiveness of Awareness Program
N = 60

Level of Knowledge	Mean Diff	Std. Deviation	t	df	Sig
Pre- Test Post- Test	7.283	5.04	11.1	59	0.00

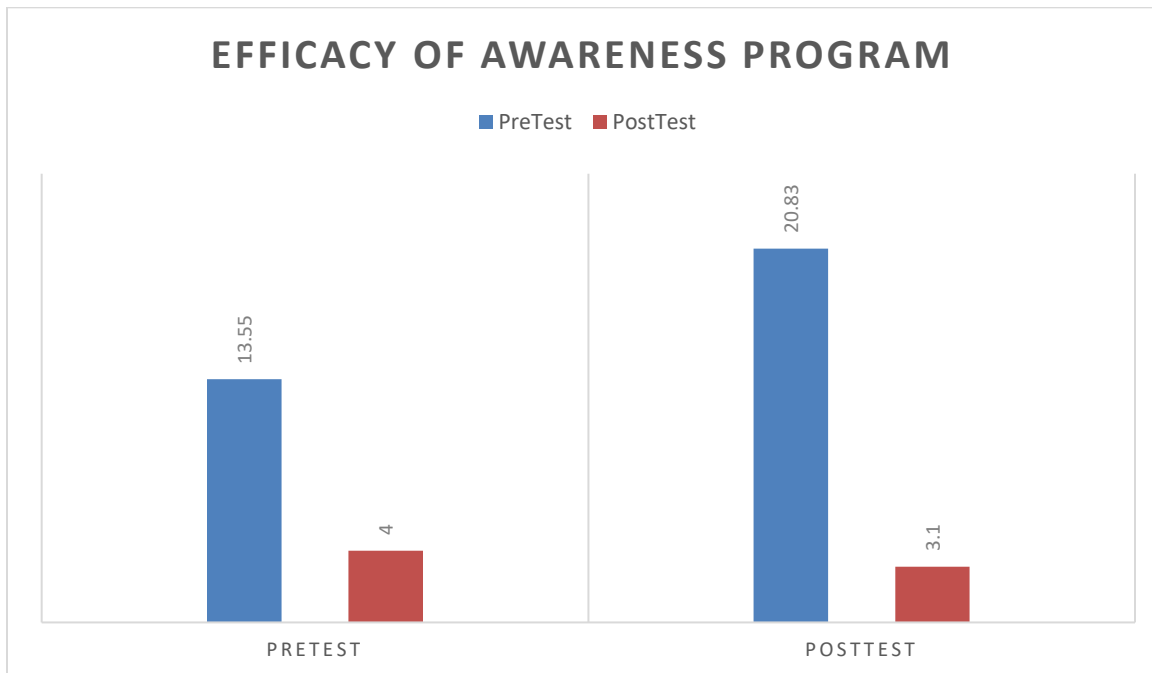


Figure 2: Bar Chart Showing Mean and Standard Deviation of Knowledge Scores

The results of a paired samples t-test used to assess how the intervention affected respondents' scores are shown in Table 3. After the intervention, the mean score rose from 13.55 (SD=4.048) to 20.83 (SD=3.147). The pre-test and post-test scores differ significantly, according to the paired samples t-test ($t(59) = -11.173$, $p < 0.001$). This suggests that the intervention was successful in raising the respondents' scores considerably.

Section D: Table 4- association between pre-test level of knowledge regarding cybercrime and its prevention with their selected demographic variables

N = 60

Demographic Variable	Category	Adequate Awareness	Inadequate Awareness	Moderate Awareness	Total	Pearson Chi-Square	df	P value
Age	10 to 12 years	0	18	4	22	7.77	4	0.10
	13 to 15 years	0	10	8	18			
	16 to 18 years	2	11	7	20			
Gender	Male	1	19	6	26	1.56	2	0.45
	Female	1	20	13	34			
Current Standard	9th - 10th Standard	2	37	16	55			

	11th - 12th Standard	0	2	3	5	2.08	2	0.35
Digital Exposure	1-2 Hours	1	24	14	39	1.8	4	0.76
	3-5 Hours	1	13	5	19			
	6-8 Hours	0	2	0	2			
Primary Device	Mobile phone	2	28	11	41	9.11	6	0.16
	Computer	0	3	1	4			
	Laptop	0	7	2	9			
	Other	0	1	5	6			
Previous Knowledge	Yes	0	5	1	6	1.04	2	0.59
	No	2	34	18	54			

Significant at 0.05 level

S = Significant, NS = Not – Significant

In order to ascertain whether baseline awareness Pre- Levels—which were primarily classified as insufficient (n=39)—were related to different demographic and background characteristics, a Pearson Chi-Square analysis was performed on a sample of 60 participants. According to the test results, there were no statistically significant correlations between the participants' awareness levels and their age ($p = .100$), gender ($p = .457$), current educational standard ($p = .352$), daily hours of digital exposure ($p = .762$), primary digital device used ($p = .167$), or claimed prior knowledge of the subject ($p = .594$). The results show that the participants' initial awareness levels are independent of their age, gender, educational background, and digital habits because all asymptotic significance values easily above the conventional 0.05 alpha criterion.

DISCUSSION

Findings related to knowledge regarding cyber-crime and its prevention among school going children - Prior to the intervention, 65.0% (n=39) of the respondents showed "Inadequate Awareness" and just 3.3% (n=2) showed "Adequate Awareness," according to the baseline results of this study, indicating a worrying lack of digital literacy among the participants.

The findings of Mousa et al. (2019), who also reported a significant lack of awareness of cyber hazards and noted that students usually demonstrated just a small, surface-level comprehension of digital vulnerabilities, are consistent with this severe lack of core cybersecurity knowledge. Additionally, the findings of Vohra A. et al. (2022) and Al-Qahtani A. et al. (2023), who both reported startlingly high rates of cyber-victimization and harassment among adolescents due to a basic lack of proactive defense mechanisms and digital literacy, strongly align with this high level of baseline vulnerability.

The participants' knowledge levels significantly improved after the educational intervention was given, with the majority (71.7%, n=43) moving up to "Moderate Awareness" and those with "Adequate Awareness" sharply increasing to 21.7% (n=13). As a result, only 6.7% (n=4) of pupils had insufficient awareness. The effectiveness of organized, school-based cybersecurity initiatives is strongly validated by this noticeable increase.

Tsimtsiou et al. (2021), who showed that interactive class presentations greatly improved teenage students' comprehension of online safety and social network usage, provide compelling evidence for the effectiveness of this pedagogical change. Furthermore, these favorable cognitive results are consistent with the findings of Ágnes Lukács et al. (2022), who found that a focused anti-cyberbullying program improved primary kids' digital awareness and defensive responses right away. In the end, this upward shift in competency emphasizes the crucial role of specialized educational interventions, supporting the findings of Klein et al. (2020), who stressed that particular IT protection knowledge serves as an essential mediator for converting fundamental comprehension into protective cybersecurity behaviors.

Findings related to Efficacy of awareness program regarding cybercrime and its prevention - The findings of the paired samples t-test unequivocally show that the cybercrime awareness intervention is effective. The structured educational program was remarkably successful in improving the respondents' understanding of cyber threats, as demonstrated by the highly significant increase in the mean knowledge score from 13.55 (SD=4.048) in the pre-test to 20.83 (SD=3.147) in the post-test ($t(59) = -11.173$, $p < 0.001$).

The substantial statistical gains achieved in this study strongly support previous research calling for formal cybersecurity training in educational settings. The remarkable increase in student knowledge mirrors the work of Tsimitsiou et al. (2021), who found that engaging, school-led presentations successfully taught teens about digital dangers and available support systems. Additionally, the measurable impact of this program aligns with Klein et al. (2020), who determined that targeted IT and cyber defense coursework is essential for pushing students past basic assumptions and into proactive, safe online habits. Finally, much like the STAnD anti-cyberbullying initiative studied by Ágnes Lukács et al. (2022)—which triggered quick, quantifiable improvements in students' defensive behaviors—the current study's strong statistical significance ($p < 0.001$) and consistent post-test scores confirm that focused educational programs are highly effective at boosting youth digital literacy.

CONCLUSION

Adolescents enrolled in school initially confront significant risks in the digital sphere, which are typified by a basic lack of proactive defensive measures and fundamental cybersecurity awareness. Regardless of the students' age, gender, educational background, or everyday digital behaviors, there remains a significant baseline deficiency in digital literacy. The pupils' comprehension of cyberthreats quickly and quantitatively improved when a planned, 45-minute interactive audio-visual lesson was implemented. Targeted pedagogical interventions successfully move teens toward safe, proactive online behaviors, as evidenced by the notable shift in the student population from insufficient awareness to moderate and adequate awareness. In order to safeguard youth in a fast-digitizing culture, official cybersecurity awareness and training programs must be established in school settings.

NURSING IMPLICATIONS

Nursing Practice: Regardless of age, gender, or level of digital exposure, pediatric, psychiatric, and school health nurses should perform organized audio-visual awareness presentations in schools and incorporate routine screening for cyber-victimization into adolescent health evaluations. Additionally, nurses should instruct parents and students on how to use reporting resources like the National Cybercrime Reporting Portal and the 1930 helpline.

Nursing Education: In order to prepare nursing students to create and present interactive audio-visual health education for young people, nursing curriculum should include courses on digital health literacy, new cyberthreats, and the psychological effects of online abuse.

Nursing Administration: In addition to allocating funds for the creation of standardized teaching resources and in-service staff training, nurse administrators should cooperate with school authorities to institutionalize recurring cybersecurity seminars into school health programs.

Nursing Research: In order to assess long-term behavioral recall and safe online habits beyond the 7-day post-test period, future research should build on this single-group design ($N = 60$) by performing multi-center randomized controlled trials with bigger samples.

LIMITATIONS

- The study employs a one-group pre-test/post-test quasi-experimental design without a control group to assess the impact of the intervention.
- All findings and statistical analyzes are predicated on a final sample size of 60 respondents, even if the protocol mentions an initial selection of 100 students.
- Because the study only included students from one particular secondary school in Dehradun, it is difficult to extrapolate the results to larger populations or other geographical areas.
- Instead of using conventional evaluation instruments or observing real digital activity, data gathering depended on a self-structured multiple-choice questionnaire to gauge awareness.

DECLARATIONS - We hereby declare that the research project entitled “understanding cybercrime awareness levels among school students: a quasi-experimental study in Dehradun is an original work done by us.

Funding - We declare that no any funding was provided for the study.

Conflict of Interest - Authors declares no any conflict of interest.

REFERENCES -

- Al Ali, N., Qasem, I. O., & Aldwaikat, T. (2025). Examining the Impact of a School-Based Bullying Education Program on Students' Knowledge of Bullying, Bullying Behavior, and Self-Esteem. *International Journal of Adolescence and Youth*, 30. <https://doi.org/10.1080/02673843.2025.2454997>
- Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, 15, 2175. <https://doi.org/10.3390/sym15122175>

- Alqahtani, M. A. (2022). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Computational Intelligence and Neuroscience*, 2022, 1–12. <https://doi.org/10.1155/2022/6775980>
- Amin, S. M., Mohamed, M. A. E., Metwally El-Sayed, M., & El-Ashry, A. M. (2024). Nursing in the digital age: The role of nursing in addressing cyberbullying and adolescents mental health. *Journal of Psychiatric and Mental Health Nursing*, 32, 57–70. <https://doi.org/10.1111/jpm.13085>
- Bansal, S., Garg, N., Singh, J., & Van Der Walt, F. (2024). Cyberbullying and mental health: past, present and future. *Frontiers in Psychology*, 14. <https://doi.org/10.3389/fpsyg.2023.1279234>
- Bickham, D. S., Moukalled, S., Inyart, H. K., & Zlokower, R. (2021). Evaluating a Middle-School Digital Citizenship Curriculum (Screenshots): Quasi-Experimental Study. *JMIR Mental Health*, 8, e26197. <https://doi.org/10.2196/26197>
- Cremer, F., Sheehan, B., Fortmann, M., et al. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47, 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, 27, 4729–4752. <https://doi.org/10.1007/s10639-021-10806-7>
- Earnshaw, V. A., Reisner, S. L., Menino, D. D., et al. (2018). Stigma-based bullying interventions: A systematic review. *Developmental Review*, 48, 178–200. <https://doi.org/10.1016/j.dr.2018.02.001>
- Gaffney, H., Ttofi, M. M., & Farrington, D. P. (2021). Effectiveness of school-based programs to reduce bullying perpetration and victimization: An updated systematic review and meta-analysis. *Campbell Systematic Reviews*, 17. <https://doi.org/10.1002/cl2.1143>
- Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security*, 29, 485–499. <https://doi.org/10.1108/ics-08-2020-0131>
- Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. *SN Social Sciences*, 2. <https://doi.org/10.1007/s43545-021-00305-4>
- Hygeia S. Toso, C., A. Jumalon, A. J., R. Magadan, J. A., B. Alvarico, A., & Cuevas Jr, J. F. (2023). Cybercrime Awareness Among Senior High School Students. *Mediterranean Journal of Basic and Applied Sciences*, 07, 160–176. <https://doi.org/10.46382/mjbas.2023.7218>
- Jackson, E., Boyes, M., Blundell, B., Hirn, J., & Leitão, S. (2025). Managing cyberbullying among adolescents with neurodevelopmental disorders: A scoping review. *International Journal of Speech-Language Pathology*, 1–16. <https://doi.org/10.1080/17549507.2025.2451305>
- Jang, Y., & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. *Children*, 10, 1415. <https://doi.org/10.3390/children10081415>
- Jun, W. (2020). A Study on the Cause Analysis of Cyberbullying in Korean Adolescents. *International Journal of Environmental Research and Public Health*, 17, 4648. <https://doi.org/10.3390/ijerph17134648>
- Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, 21, 129–137. <https://doi.org/10.1089/cyber.2016.0728>
- Kaakinen, M., Koivula, A., Savolainen, I., et al. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. *Aggressive Behavior*, 47, 530–543. <https://doi.org/10.1002/ab.21968>
- Kumar, V. L., & Goldstein, M. A. (2020). Cyberbullying and Adolescents. *Current Pediatrics Reports*, 8, 86–92. <https://doi.org/10.1007/s40124-020-00217-6>
- Kwan, I., Dickson, K., Richardson, M., et al. (2020). Cyberbullying and Children and Young People's Mental Health: A Systematic Map of Systematic Reviews. *Cyberpsychology, Behavior, and Social Networking*, 23, 72–82. <https://doi.org/10.1089/cyber.2019.0370>
- Lukács J., Á., Takács, J., Soósne Kiss, Z., et al. (2022). The Effects of a Cyberbullying Intervention Programme Among Primary School Students. *Child & Youth Care Forum*, 52, 893–911. <https://doi.org/10.1007/s10566-022-09714-9>
- Monteith, S., Bauer, M., Alda, M., et al. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, 23. <https://doi.org/10.1007/s11920-021-01228-w>
- Palladino, B. E., Nocentini, A., & Menesini, E. (2016). Evidence-based intervention against bullying and cyberbullying: Evaluation of the NoTrap! program in two independent trials. *Aggressive Behavior*, 42, 194–206. <https://doi.org/10.1002/ab.21636>
- Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. *PeerJ Computer Science*, 8, e918. <https://doi.org/10.7717/peerj-cs.918>

- Rahman, T., Hossain, M. M., Bristy, N. N., Hoque, M. Z., & Hossain, M. M. (2023). Influence of cyber-victimization and other factors on depression and anxiety among university students in Bangladesh. *Journal of Health, Population and Nutrition*, 42. <https://doi.org/10.1186/s41043-023-00469-0>
- Ranjith, P. J., Vranda, M. N., & Kishore, M. T. (2023). Predictors, prevalence, and patterns of cyberbullying among school-going children and adolescents. *Indian Journal of Psychiatry*, 65, 720–728. https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_313_23
- Ranjith, P. J., Vranda, M. N., & Kishore, M. T. (2025). Development and validation of school-based intervention on cyberbullying for adolescents. *Indian Journal of Psychiatry*, 67, 252–255. https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_777_23
- Tsimtsiou, Z., Drosos, E., Drontsos, A., et al. (2017). Raising awareness on cyber safety: adolescents' experience of a primary healthcare professional-led, school-based, multi-center intervention. *International Journal of Adolescent Medicine and Health*, 31. <https://doi.org/10.1515/ijamh-2017-0072>
- Yosep, I., Pramukti, I., Agustina, H. R., et al. (2022). Triple-P e-Parenting to Improve Awareness of Psychiatric Nurses on Preventing Cyberbullying in Adolescents. *Healthcare*, 11, 19. <https://doi.org/10.3390/healthcare11010019>
- Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health*, 9. <https://doi.org/10.3389/fpubh.2021.634909>