



CYBERSECURITY AWARENESS, CYBER HUMAN VALUES AND CYBERBULLYING BEHAVIOUR AMONG UNDERGRADUATE STUDENTS: AN EMPIRICAL STUDY

Dr. Nayana L M¹, Mr. Shravan S Kulal²

¹Associate Professor of Commerce, Govt. First Grade College for Women, Balmatta, Mangalore 575001.

²M.Com (Final), Govt. First Grade College & PG Study Center, Kaup, Udupi District 574106.

Article DOI: <https://doi.org/10.36713/epra31367>

DOI No: 10.36713/epra31367

ABSTRACT

The increasing use of digital technologies and social media among young adults has created a growing need for safe, ethical and responsible online behaviour. In this context, cybersecurity awareness and cyber human values play an important role in shaping individuals' online behaviour and may influence their involvement in cyberbullying. The present study examines cybersecurity awareness, cyber human values and cyberbullying behaviour among undergraduate students in Udupi district. The study adopted a descriptive research design using a quantitative approach. Primary data were collected from 109 undergraduate students pursuing B.Com, BBA, BA, BCA and B.Sc programmes through a structured questionnaire using convenience sampling. Secondary data were collected from books, journals, research articles, websites and previous studies. The collected data were analysed using percentage analysis, mean, standard deviation, correlation analysis and the Chi-square test. The findings indicate that undergraduate students possess a good level of cybersecurity awareness and knowledge of online security and cyber safety practices. The study also reveals that students demonstrate positive cyber human values, although there is scope for further strengthening ethical and responsible digital behaviour. Further, cybersecurity awareness is found to be significantly associated with cyberbullying behaviour, while cyber human values also show a significant association with cyberbullying. The findings additionally indicate a significant positive relationship between cybersecurity awareness and cyber human values, suggesting that greater awareness of cybersecurity may be associated with stronger ethical values in the digital environment. The study highlights the need for higher educational institutions to strengthen cybersecurity education, digital ethics and responsible online behaviour through awareness programmes, curriculum-based interventions and student-oriented digital citizenship initiatives.

KEYWORDS: Cybersecurity Awareness, Cyber Human Values, Cyberbullying, Online Safety, Ethical Digital Behaviour

INTRODUCTION

The rapid development of digital technology has changed the way people communicate, learn, socialize, and share information. The internet, smartphones, social media platforms, online games, and digital communication tools have become part of everyday life, especially among students. Students use digital technology for academic purposes, entertainment, communication, banking, shopping, and social networking. Although technology provides many benefits, it also creates several challenges related to online safety, digital ethics, and harmful online behaviour.

In recent years, cybersecurity awareness has become an important issue across the world. Many students spend a large amount of time online but may not fully understand the risks related to cyber threats such as hacking, phishing, identity theft, malware attacks, cyber fraud, online scams, privacy breaches, and cyberbullying. A lack of cybersecurity awareness may expose students to different forms of online victimization and risky online behaviour.

At the same time, cyber human values have become important in the digital environment. Cyber human values refer to ethical values, responsible behaviour, respect, empathy, honesty, integrity, digital responsibility, and proper communication in online spaces. Students who practice positive cyber human values are more likely to behave responsibly online and avoid harmful actions toward others.

Another growing issue in the digital world is cyberbullying. Cyberbullying refers to the use of digital technology to harass, threaten, insult, embarrass, or harm others through online platforms. It can occur through social media, text messages, emails, online games, discussion forums, or fake accounts. Cyberbullying has become a major concern among undergraduate students because it negatively affects mental health, emotional well-being, academic performance, and social relationships.

This study focuses on examining the level of cybersecurity awareness among undergraduate students, identifying their cyber human values, analysing the prevalence of cyberbullying, and examining the relationship between these variables. The study aims to provide useful information for educational institutions, students, parents, policymakers, and researchers in creating safer and more ethical digital environments.

OBJECTIVES OF THE STUDY

- To examine the level of cybersecurity awareness among undergraduate students.
- To identify the level of cyber human values among undergraduate students.
- To analyse the prevalence of cyberbullying experience among undergraduate students.



- To examine the relationship between cybersecurity awareness, cyber human values, and cyberbullying behaviour among students

RESEARCH HYPOTHESIS

Hypothesis 1

H01: There is no significant relationship between Cybersecurity Awareness and Cyberbullying among undergraduate students.

H11: There is a significant relationship between Cybersecurity Awareness and Cyberbullying among undergraduate students.

Hypothesis 2

H02: There is no significant relationship between Cyber Human Values and Cyberbullying among undergraduate students.

H12: There is a significant relationship between Cyber Human Values and Cyberbullying among undergraduate students.

Hypothesis 3

H03: There is no significant relationship between Cybersecurity Awareness and Cyber Human Values among undergraduate students.

H13: There is significant relationship between Cybersecurity Awareness and Cyber Human Values among undergraduate students.

LIMITATIONS OF THE STUDY

Every research study has certain limitations. This study also has following limitations.

1. The study focuses only on undergraduate students, therefore, the findings may not represent other groups such as school students or postgraduate students.
2. The study depends on self-reported responses from participants. Some students may provide socially acceptable answers instead of honest responses.
3. The study may be limited to selected colleges or universities, which may affect the generalization of findings.
4. Cyberbullying experiences may vary depending on individual backgrounds, culture, and social media usage.
5. The study focuses only on selected variables and may not include other factors such as family background, peer influence, personality, or psychological conditions.

REVIEW OF LITERATURE

The growing dependence of undergraduate students on digital platforms has increased the importance of cybersecurity awareness, responsible online behaviour and cyber human values. The reviewed literature indicates that although students generally possess basic knowledge of cyber threats, significant gaps remain between awareness, ethical understanding and actual online practices. Verma and Devi (2026) found a positive relationship between cybercrime awareness and human rights awareness among college students, suggesting that greater awareness of cyber threats is associated with more responsible online behaviour and ethical decision-making. Similarly, Ering et al. (2025) reported that undergraduate students were generally familiar with common threats such as phishing, identity theft and online fraud, but their knowledge of advanced cybersecurity measures was limited. The study emphasized the need to strengthen cyber literacy through regular training and curriculum-based awareness programmes.

A recurring finding in the literature is the gap between cybersecurity awareness and actual protective behaviour. Hazarika, H. J. (2025) found that although many undergraduate students were aware of cyber threats, they did not always adopt adequate security measures. Experiences of account hacking, phishing and privacy violations highlighted the vulnerability of students, particularly in social media environments. Begum, N. (2024) similarly observed that students possessed basic awareness of cyber risks but had comparatively lower knowledge of privacy protection, password security and cyber ethics. Students who had participated in cyber awareness programmes demonstrated better knowledge and safer online practices. These findings indicate that awareness programmes need to move beyond theoretical knowledge and develop practical cybersecurity skills.

The literature further establishes that cybersecurity awareness alone may not be sufficient to ensure responsible digital behaviour. Nurse (2021) emphasized that cybersecurity awareness becomes meaningful when it results in behavioural change and identified human behaviour as a critical element of cybersecurity. Kshetri, Vasudha and Hoxha (2023) found that Computer Science students possessed greater technical knowledge than non-Computer Science students, but deficiencies in cyber ethics were evident in both groups. The study emphasized that technical cybersecurity knowledge needs to be complemented by ethical values such as honesty, respect and responsibility. Thus, cybersecurity education should incorporate both technical awareness and ethical dimensions of digital citizenship.

An important dimension emerging from the literature is the relationship between cyber human values and cyberbullying. Cheong Shun Xiang and Hasbullah (2023), in their study of university students in Selangor, Malaysia, examined cybersecurity awareness, cyber human values and cyberbullying. The findings showed significant relationships between cybersecurity awareness, cyber human values and cyberbullying behaviour. Students with stronger cyber human values were less likely to engage in cyberbullying, while password security awareness was identified as a significant predictor of cyberbullying. The study consequently emphasized the need to integrate cybersecurity awareness with ethical online behaviour and digital values.

Previous research has also identified empathy, respect, responsibility and ethical behaviour as important protective factors against cyberbullying. Al-Romaihi and Ikuesan (2022) found that aggressive online behaviour can act as an indicator of cyberbullying and



emphasized the importance of empathy, respect and ethical values in preventing online harassment. Patchin and Hinduja (2018) similarly highlighted digital citizenship, awareness and cyber human values as important elements of cyberbullying prevention. These studies suggest that cyberbullying should not be viewed solely as a technological or disciplinary problem; it also reflects the ethical and social values that students apply in digital environments.

The literature also highlights the prevalence and consequences of cyberbullying among students. Chauhan (2019) found that a significant proportion of undergraduate students had experienced or witnessed cyberbullying, with social media and messaging applications identified as common platforms. Erişti and Akbulut (2018) found that students experiencing cyberbullying often responded by ignoring the incident rather than reporting it, partly because of limited awareness of available support systems. Faucher, Cassidy and Jackson (2020) found that university students identified awareness campaigns, privacy controls, institutional policies and accessible reporting systems as important measures for addressing cyberbullying. These findings demonstrate that cybersecurity education should incorporate not only prevention but also mechanisms for responding to cyberbullying and supporting affected students.

The reviewed literature further points to the importance of institutional responsibility and a comprehensive educational approach. Lallie et al. (2023) identified phishing, ransomware and data breaches as important cyber threats to educational institutions and emphasized that students and faculty can be vulnerable because of inadequate cybersecurity awareness. Cross et al. (2015) highlighted the influence of individual, social and environmental factors on cyberbullying and argued for a social-ecological approach involving students, families and educational institutions. El Asam and Samara (2016) further emphasized the importance of awareness of cyber law and students' digital rights and responsibilities. These findings suggest that universities need comprehensive cybersecurity policies, regular awareness programmes, ethical education, reporting mechanisms and support systems.

Overall, the reviewed literature establishes that cybersecurity awareness, cyber human values and cyberbullying are interconnected dimensions of students' digital behaviour. Awareness of cyber threats can contribute to safer online practices, while cyber human values such as empathy, respect, honesty and responsibility can discourage harmful online behaviour. At the same time, inadequate awareness, weak ethical understanding and inappropriate online conduct can increase students' vulnerability to cyber risks and cyberbullying. The literature therefore supports an integrated approach that combines technical cybersecurity knowledge with cyber ethics, digital citizenship and responsible online behaviour.

However, the reviewed studies also reveal scope for further empirical research, particularly among undergraduate students in specific educational and geographical contexts. While several studies have examined cybersecurity awareness or cyberbullying independently, relatively fewer studies have considered cybersecurity awareness, cyber human values and cyberbullying together as interconnected dimensions of students' digital behaviour. The present study therefore seeks to examine these dimensions among undergraduate students and contribute to a better understanding of how cybersecurity knowledge and ethical cyber values relate to cyberbullying behaviour in the higher education context.

RESEARCH METHODOLOGY

The present study focuses on cybersecurity awareness, cyber human values, and cyberbullying among undergraduate students. The study aims to understand the level of cybersecurity awareness among students, identify their cyber human values, analyse the prevalence of cyberbullying, and examine the relationship between cybersecurity awareness, cyber human values, and cyberbullying behaviour.

The present study adopted a descriptive research design using a quantitative research approach. The study focuses only on undergraduate students studying in colleges located in Udupi district. 109 students were selected as respondents for the study to examine cybersecurity awareness, cyber human values, and cyberbullying among undergraduate students.

Distribution of respondents:

Course	Number of Respondents
B. Com	36
BBA	21
BA	22
BCA	24
BSC	06
Total	109

The present study used the convenience sampling technique. Under this method, respondents who were easily available and willing to participate were selected for the study. The study used both primary data and secondary data. primary data was collected through a structured questionnaire distributed among undergraduate students. The questionnaire included questions related to Cybersecurity awareness, Cyber human values, Cyberbullying behaviour. Secondary data for the study was collected from Books, Journals, Research articles, Websites, Previous research studies, Academic publications. The collected data was analysed using statistical tools such as percentage analysis, mean and standard deviation, correlation analysis and Chi-square test.



DATA ANALYSIS AND INTERPRETATION

1. Demographic Profile of Respondents

The demographic characteristics of the respondents were analysed to understand the background of the participants included in the study. The variables considered for demographic analysis were gender, course/stream, year of study, average daily internet usage, and primary device used for internet access. The frequency and percentage distribution of respondents for each demographic variable are presented in the table below.

Table No 1.1: Demographic Analysis

Demographic Analysis			
		Frequency	Percentage
Gender	Male	60	55.00
	Female	49	45.00
	Other	0	0
	Total	109	100.00
Course/Stream	BA	22	20.02
	BCom	36	33.00
	BSc	6	5.05
	BCA	24	22.00
	BBA	21	19.03
	Total	109	100.00
Year of Study	1 st Year	28	25.07
	2 nd Year	36	33.00
	3 rd Year	45	41.03
	Total	109	100.00
Average daily internet usage	Less Than 2 Hours	8	7.03
	2-4 Hours	48	44.00
	4-6 Hours	42	38.05
	More Than 6 Hours	11	10.01
	Total	109	100.00
Primary device used	Smartphones	83	76.14
	Laptop	24	22.01
	Tablet	1	0.917
	Desktop	1	0.917
	Total	109	100.00

Sources: Survey Data

- Male respondents formed the majority of the study participants. Female respondents also constituted a substantial portion of the sample, ensuring balanced representation.
- BCom students formed the largest group of respondents in the study. BCA students constituted the second-largest group, followed closely by BA and BBA students. BSc students represented the smallest group among the respondents.
- Third-year students formed the largest group of respondents in the study. Second-year students constituted the second-largest group, followed by first-year students.
- Most respondents used the internet for 2–4 hours per day, making it the most common usage category. A large number of students also reported using the internet for 4–6 hours daily, indicating high online engagement. Only a small number of respondents used the internet for less than 2 hours or more than 6 hours per day.
- Smartphones were the most commonly used device among the respondents for accessing the internet and digital services. Laptops were the second most preferred device, particularly for academic and educational activities. Very few respondents reported using tablets or desktop computers as their primary device.

1. Descriptive Statistics of Cybersecurity Awareness, Cyber Human Values and Cyberbullying

Table No 1.2.1 Cybersecurity Awareness

	N	Missing	Mean	Median	SD	Variance	Minimum	Maximum
CSA SCORE	109	0	3.85	4.00	0.759	0.576	1.00	5.00

Sources: Survey Data

Interpretation of Cybersecurity Awareness Score (CSA)

The descriptive statistics indicate that the Cybersecurity Awareness (CSA) Score of the 109 undergraduate students has a mean value of 3.85 and a median value of 4.00. This suggests that the respondents possess a relatively high level of cybersecurity awareness.



The median score being slightly higher than the mean indicates that most students scored around the higher end of the scale. The standard deviation of 0.759 shows that the responses are moderately dispersed around the mean, indicating some variation in cybersecurity awareness levels among the students. The variance of 0.576 further supports this finding.

The minimum score of 1.00 and the maximum score of 5.00 indicate that the full range of the scale was utilized by the respondents, showing the presence of both low and high levels of cybersecurity awareness within the sample.

Overall, the findings suggest that undergraduate students demonstrate a good level of cybersecurity awareness, although differences in awareness levels exist among individual respondents.

Table No 1.2.2 Cyber Human values

	N	Missing	Mean	Median	SD	Variance	Minimum	Maximum
CHV SCORE	109	0	3.35	3.33	0.818	0.669	1.00	5.00

Sources: Survey Data

Interpretation of Cyber Human Values

The descriptive statistics indicate that the Cyber Human Values (CHV) Score of the 109 undergraduate students has a mean value of 3.35 and a median value of 3.33. This suggests that the respondents demonstrate a moderate level of cyber human values in their online behaviour and interactions.

The standard deviation of 0.818 indicates a moderate variation in the responses, showing that students differ somewhat in their levels of cyber human values. The variance of 0.669 further reflects this variability among the respondents.

The minimum score of 1.00 and the maximum score of 5.00 show that the entire range of the measurement scale was used, indicating the presence of both low and high levels of cyber human values among the students.

Overall, the findings suggest that undergraduate students possess a moderate level of cyber human values, indicating that while many students exhibit positive ethical and responsible behaviour in digital environments, there is still room for improvement in promoting stronger cyber human values among the student population.

Table No 1.2.3 Cyberbullying

	N	Mean	Median	SD	Variance	Minimum	Maximum
CB SCORE	109	3.09	3.33	0.869	0.755	1.00	4.50

Sources: Survey Data

Interpretation of Cyberbullying

The descriptive statistics for the Cyberbullying (CB) scores of the 109 undergraduate students revealed a mean score of 3.09 and a median score of 3.33, indicating a moderate level of cyberbullying-related experiences or behaviour among the respondents. The standard deviation of 0.869 and variance of 0.755 suggest a moderate degree of variability in cyberbullying scores, reflecting differences in students' experiences and behaviours related to cyberbullying. Furthermore, the scores ranged from a minimum of 1.00 to a maximum of 4.50, demonstrating that respondents reported varying levels of cyberbullying, from very low to relatively high.

Overall, the findings indicate that cyberbullying exists at a moderate level among undergraduate students. These results emphasize the importance of implementing awareness programs, promoting responsible online behaviour, and encouraging digital ethics to help reduce cyberbullying and create a safer online environment for students.



2. Testing of hypotheses Cybersecurity Awareness, Cyber Human Values and Cyberbullying

Table No 1.3.1 Correlation Between Cybersecurity Awareness and Cyberbullying

		CSA SCORE	CB SCORE
CSA SCORE	Pearson's r	—	
	df	—	
	p-value	—	
CB SCORE	Pearson's r	0.516***	—
	df	107	—
	p-value	<.001	—
Note. * $p < .05$, ** $p < .01$, *** $p < .001$			

Sources: Survey Data

Interpretation

A Pearson correlation analysis was conducted to examine the relationship between Cybersecurity Awareness (CSA) and Cyberbullying (CB) among undergraduate students. The results revealed a moderate positive correlation between CSA and CB scores, $r(107) = 0.516$, $p < .001$. This finding indicates a statistically significant relationship between cybersecurity awareness and cyberbullying.

Hence, the null hypothesis was rejected, and it was concluded that cybersecurity awareness is significantly associated with cyberbullying among undergraduate students.

Table No 1.3.2 Correlation between Cyber Human Values and cyberbullying

		CHV SCORE	CB SCORE
CHV SCORE	Pearson's r	—	
	df	—	
	p-value	—	
CB SCORE	Pearson's r	0.468***	—
	df	107	—
	p-value	<.001	—
Note. * $p < .05$, ** $p < .01$, *** $p < .001$			

Sources: Survey Data

Interpretation

The Pearson correlation analysis was conducted to examine the relationship between Cyber Human Values (CHV) and Cyberbullying (CB) among undergraduate students. The results indicated a moderate positive correlation between CHV scores and CB scores ($r = 0.468$, $p < .001$). Since the p -value is less than 0.001, the relationship is statistically significant.

Therefore, the null hypothesis (H_0) was rejected and the alternative hypothesis (H_1) was accepted. It can be concluded that there is a significant relationship between Cyber Human Values and Cyberbullying among undergraduate students.

Table No 1.3.3 Correlation between Cybersecurity Awareness and Cyber Human Values.

		CSA SCORE	CHV SCORE
CSA SCORE	Pearson's r	—	
	df	—	
	p-value	—	
CHV SCORE	Pearson's r	0.604***	—
	df	107	—
	p-value	<.001	—
Note. * $p < .05$, ** $p < .01$, *** $p < .001$			

Sources: Survey Data

Interpretation

To examine the relationship between Cybersecurity Awareness and Cyber Human Values among undergraduate students, a Pearson correlation analysis was conducted. The results showed a strong positive correlation between CSA scores and CHV scores ($r = 0.604$, $p < .001$). Since the p -value is less than 0.001, the relationship is statistically significant.

Therefore, the null hypothesis (H_0) was rejected and the alternative hypothesis (H_1) was accepted. It is concluded that there is a significant positive relationship between Cybersecurity Awareness and Cyber Human Values among undergraduate students.

FINDINGS

- The findings suggest that undergraduate students possess good knowledge and awareness of online security and cyber safety practices.
- The study indicates that while students possess positive cyber human values, there is scope for further improvement in promoting ethical online behaviour.



- The findings suggest that Cybersecurity Awareness is significantly associated with Cyberbullying among undergraduate students.
- The study confirms that Cyber Human Values are significantly associated with Cyberbullying among undergraduate students.
- The findings confirm that students with higher Cybersecurity Awareness tend to demonstrate stronger Cyber Human Values.

SUGGESTIONS AND RECOMMENDATIONS

Based on the findings of the study, the following suggestions and recommendations are proposed for various stakeholders involved in promoting safe, ethical and responsible digital behaviour among undergraduate students.

1. Suggestions for Students

1. **Strengthen responsible online behaviour:** Students should translate their existing cybersecurity knowledge into consistent safe and ethical online practices rather than limiting awareness to theoretical knowledge.
2. **Develop stronger cyber human values:** Students should consciously practise values such as empathy, respect, honesty, responsibility, tolerance and kindness while communicating through social media, messaging applications and other digital platforms.
3. **Avoid cyberbullying and harmful communication:** Students should refrain from posting, forwarding, commenting on or sharing content that may humiliate, threaten, harass or emotionally harm others.
4. **Report cyberbullying:** Students who experience or witness cyberbullying should make use of appropriate institutional reporting mechanisms rather than ignoring such incidents.

2. Suggestions for College Administration

1. **Conduct regular cybersecurity awareness programmes:** Colleges should organize workshops, seminars and training programmes on cyber safety, online privacy, phishing, identity theft, password security and other relevant cyber threats.
2. **Integrate cyber human values into student development programmes:** Since cyber human values are significantly associated with cyberbullying, colleges should include empathy, respect, responsibility, ethical communication and digital citizenship in student orientation and value-education programmes.
3. **Develop a clear anti-cyberbullying policy:** Colleges should formulate clear guidelines defining unacceptable online behaviour and specify appropriate procedures for reporting and addressing cyberbullying incidents.
4. **Establish confidential reporting mechanisms:** Students should have access to safe and confidential mechanisms for reporting cyberbullying, online harassment and other cyber-related incidents.
5. **Provide counselling and support:** Colleges should provide appropriate counselling and support to students affected by cyberbullying and create an environment in which students feel comfortable seeking assistance.

3. Suggestions for Parents

1. **Maintain open communication with students:** Parents should encourage students to discuss their online experiences, including uncomfortable or threatening interactions, without fear of blame or punishment.
2. **Promote ethical digital behaviour:** Parents should guide students to practise respect, empathy, responsibility and appropriate communication in digital environments.
3. **Create awareness about cyber risks:** Parents should familiarize themselves with common cyber threats and encourage students to follow safe online practices.
4. **Monitor constructively:** Parents should provide appropriate guidance regarding digital activities while respecting the growing independence and privacy of undergraduate students.
5. **Encourage reporting rather than silence:** Students should be encouraged to seek help when they experience or witness cyberbullying instead of ignoring the problem.

4. Suggestions for Government and Educational Authorities

1. **Strengthen cybersecurity education in higher education:** Government and educational authorities should encourage the inclusion of cybersecurity awareness and digital citizenship in undergraduate education.
2. **Develop standard awareness programmes:** Common educational resources on cybersecurity, cyber ethics, cyber human values and cyberbullying can be developed for use across colleges.
3. **Promote cyberbullying awareness campaigns:** Awareness campaigns should explain the forms, consequences and prevention of cyberbullying and encourage responsible digital communication.
4. **Strengthen student support mechanisms:** Educational authorities should encourage institutions to establish accessible mechanisms for reporting cyberbullying and other cyber-related concerns.
5. **Encourage digital citizenship initiatives:** Government programmes should promote responsible and ethical use of digital technologies alongside technical cybersecurity awareness.

CONCLUSION

Overall, the study concludes that developing a cyber-safe and ethically responsible student community requires an integrated approach to cybersecurity awareness, cyber human values and cyberbullying prevention. Regular awareness programmes, practical cybersecurity training, digital ethics education, effective reporting mechanisms and institutional support can contribute to safer



online environments for undergraduate students. The combined efforts of students, educational institutions, parents, government and policymakers are therefore essential for developing responsible digital citizens and reducing harmful online behaviour among young adults.

REFERENCES

1. Abaido, G. M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, 25(1), 407–420. <https://doi.org/10.1080/02673843.2019.1669059>
2. Akbulut, Y., & Eristi, B. (2011). Cyberbullying and victimisation among Turkish university students. *Australasian Journal of Educational Technology*, 27(7), 1155–1170. <https://doi.org/10.14742/ajet.910>
3. Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Aljarboa, N. A., Kamin, Y. B., & Saud, M. S. B. (2019). How cyber stalking and cyber bullying affect students' open learning. *IEEE Access*, 7, 20199–20210. <https://doi.org/10.1109/ACCESS.2019.2891853>
4. Al-Romaihi, S. K., & Ikuesan, R. A. (2022). Cyberbullying indicator as a precursor to a cyber construct development [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2203.16869>
5. Alipan, A., Skues, J. L., Theiler, S., & Wise, L. (2020). Defining cyberbullying: A multifaceted definition based on the perspectives of emerging adults. *International Journal of Bullying Prevention*, 2, 79–92. <https://doi.org/10.1007/s42380-019-00018-6>
6. Athanasiou, K., Melegkovits, E., Andrie, E. K., Magoulas, C., Tzavara, C. K., Richardson, C., & others. (2018). Cross-national aspects of cyberbullying victimization among 14–17-year-old adolescents across seven European countries. *BMC Public Health*, 18, Article 800. <https://doi.org/10.1186/s12889-018-5682-4>
7. Barlett, C. P. (2015). Anonymously hurting others online: The effect of anonymity on cyberbullying frequency. *Psychology of Popular Media Culture*, 4(1), 70–79. <https://doi.org/10.1037/a0034335>
8. Begum, N. (2024). Cyber safety consciousness among the students pursuing higher education: A study of selected colleges and universities in Bengaluru – the capital city of Karnataka. *Indian Journal of Public Administration*, 70(3), 579–592. <https://doi.org/10.1177/00195561241271582>
9. Cassidy, W., Faucher, C., & Jackson, M. (2017). Adversity in university: Cyberbullying and its impacts on students, faculty and administrators. *International Journal of Environmental Research and Public Health*, 14(8), Article 888. <https://doi.org/10.3390/ijerph14080888>
10. Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 20, 133–155. <https://doi.org/10.23962/10539/23572>
11. Chauhan, A. (2019). A comparative study of cyber bullying among undergraduate students. *International Journal of Indian Psychology*, 7Cross, D., Lester, L., Barnes, A., Cardoso, P., & Hadwen, K. (2015). A longitudinal study of the social and emotional predictors and consequences of cyber and traditional bullying victimisation. *International Journal of Public Health*, 60, 207–217.
12. Ering, O., Ering, M., & Rajhans, R. (2025). Cybercrime awareness among undergraduate students: A descriptive study. *International Journal of Scientific Research in Science and Technology*, 12(2), 1346–1352. <https://doi.org/10.32628/IJSRST251222733>
13. El Asam, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*, 65, 127–141.
14. Faucher, C., Jackson, M., & Cassidy, W. (2014). Cyberbullying among university students: Gendered experiences, impacts, and perspectives. *Education Research International*, 2014, Article 698545. <https://doi.org/10.1155/2014/698545>
15. Faucher, C., Jackson, M., & Cassidy, W. (2015). When online exchanges bite: An examination of the policy environment governing cyberbullying at the university level. *The Canadian Journal of Higher Education*, 45(1), 102–121. <https://doi.org/10.47678/cjhe.v45i1.184215>
16. Faucher, C., Cassidy, W., & Jackson, M. (2015). From the sandbox to the inbox: Comparing the acts, impacts, and solutions of bullying in K–12, higher education, and the workplace. *Journal of Education and Training Studies*, 3(6), 111–125. <https://doi.org/10.11114/jets.v3i6.1033>
17. Francisco, S. M., Simão, A. M. V., Ferreira, P. C., & Martins, M. J. D. (2015). Cyberbullying: The hidden side of college students. *Computers in Human Behavior*, 43, 167–182. <https://doi.org/10.1016/j.chb.2014.10.045>
18. Hazarika, H. J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria: The Journal of National and International Library and Information Issues*. Advance online publication. <https://doi.org/10.1177/09557490251340833>
19. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10), Article 417. <https://doi.org/10.3390/info12100417>
20. Kshetri, N., Vasudha, & Hoxha, D. (2023). Knowledge, awareness of computer & cyber ethics between CS and non-CS university students. In 2023 IEEE International Conference on Computer Science and Education (ICCSE) (pp. 1–7). IEEE. <https://doi.org/10.1109/ICCSE57933.2023.10234567> (doi.org in Bing)
21. Nurse, J. R. C. (2021). Cybersecurity awareness: The importance of understanding human behaviour. *Computers & Security*, 110, Article 102420.
22. Patchin, J. W., & Hinduja, S. (2018). *Words wound: Delete cyberbullying and make kindness go viral*. Free Spirit Publishing.
23. Verma, R., & Devi, R. (2026). A correlational study of cyber crime awareness and human rights awareness of male and female students of college level. *International Journal of Research and Innovation in Social Science*, 10(1), 7687–7692. <https://doi.org/10.47772/IJRISS.2026.10100597>
24. Xiang, C. S., & Hasbullah, M. (2023). Cybersecurity awareness, cyber human values and cyberbullying among university students in Selangor, Malaysia. *International Journal of Advanced Research in Technology and Innovation*, 5(2), 1–11. <https://doi.org/10.55057/ijarti.2023.5.2.1>



25. Yıldız Durak, H. (2019). *Cyber human values displayed by university students in online social networking sites: The relationship of cyber human values to cyberbullying and cyber victimization behaviors displayed*. In *INTED2019 Proceedings* (pp. 10035–10038). IATED. <https://doi.org/10.21125/inted.2019.2425>
26. Zych, I., Ortega-Ruiz, R., & Del Rey, R. (2015). *Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention*. *Aggression and Violent Behavior*, 23, 1–21. <https://doi.org/10.1016/j.avb.2015.10.001>