

Cyber Safety Awareness and Digital Risk Perception among College Students in Coimbatore City

Ms. Priyanka J¹ (24phecf003@avinuty.ac.in), Research Scholar & Corresponding Author

Dr. Malarvizhi V² (malarvizhi_eco@avinuty.ac.in);  <https://orcid.org/0000-0001-9731-1902>; Professor & Head,
1 & 2: Department of Economics, Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India



Copyright: © 2026 by the authors. Licensee [The RCSAS \(ISSN: 2583-1380\)](http://www.thercsas.com). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution Non-Commercial 4.0 International License. (<https://creativecommons.org/licenses/by-nc/4.0/>). **Crossref/DOI:** <https://doi.org/10.55454/rcsas.6.10.2026.002>

Abstract: Cybercrime has become a significant concern for college students as their reliance on digital platforms continues to expand, thereby establishing cybersecurity awareness as a critical necessity for safeguarding personal information and mitigating online vulnerabilities. Government initiatives and public awareness campaigns serve a vital function in advancing secure online conduct and enhancing students' comprehension of cybersecurity threats. The research objectives encompassed examine the socioeconomic characteristics of participants, assessing awareness levels regarding social media utilization among college students, and evaluating students' satisfaction with cybersecurity legislation. The study sample comprised 111 college students recruited through Google Forms utilizing a purposive sampling methodology. Data analysis employed frequency distributions, percentage calculations, Chi-square testing, one-way ANOVA, factor analysis, and structural equation Modelling (SEM). Findings indicate that the majority of participants are young, active digital platform users who demonstrated relatively elevated awareness of social media practices and safety protocols. However, overall satisfaction remained moderate, attribute to factors including insufficient knowledge of legal frameworks, operational challenges, and inadequate institutional support systems. The research concludes that although awareness and perceived protection have progressed, a notable disparity persists between, theoretical knowledge and practical implementation of cybersecurity measures and legal safeguards among women.

Keywords: Coimbatore City, College Students, Cyber Safety, Cybersecurity, Digital Awareness, Online Risks

Article History: Received: 13 Oct- 2026; Accepted: 20 Oct- 2026; Published/Available Online: 30 Oct- 2026

1. Introduction

Digital technologies have assumed a fundamental role in educational settings, with the internet now functioning as an integral component of students' academic and social engagement. Students leverage digital platforms for research, interpersonal communication, and knowledge acquisition; however, this utilization simultaneously exposes them to online fraud schemes, breaches of data confidentiality, and detrimental online conduct including cyberbullying. Consequently, awareness of cybersecurity principles and adherence to secure online practices have become increasingly critical. The manner in which students conceptualize cybersecurity directly influences their online behavioral patterns, and research by Ahmed et al., (2024) demonstrates that students' perspectives regarding cybersecurity substantially impact their capacity to mitigate online threats. Numerous internet users, particularly contemporary college students who have developed within digital environments, lack awareness of the dangers associated with insecure online conduct to their personal information. Kim (2023) observes that, contrary to conventional assumptions, individuals who extensively utilize digital technologies frequently possess minimal understanding of cybersecurity measures and preventative strategies. While physical safety and asset security constitute priorities for the majority of individuals, the protection of digital information and virtual assets remains comparatively uncommon (Moallem, 2017). As technological advancement permeates educational, communicative, and entertainment sectors, cybercriminal activities have escalated substantially and emerged as a worldwide concern (Mohd Zubair, 2026). Students, functioning as the most prominent participants in digital platform usage, represents a particularly vulnerable demographic. Cybercriminal activities additionally generate substantial economic losses on a global scale and constitute a significant risk to public safety and financial sustainability (Nilupu et al., 2024; Sarathachandra et al., 2016). Individuals aged 18 to 25 demonstrate heightened vulnerability to online scams, including phishing attacks, hacking incidents, and cyberbullying, attributable to their extensive network engagement; consequently, parents and mentors are instrumental in fostering secure online conduct (Mohd Zubair, 2026). Cybersecurity encompasses not merely technological infrastructure but also the manner in which individuals engage with online platforms, a factor contingent upon their comprehension and behavioral patterns (Kuhail et al., 2023; Moallem, 2018). Awareness levels remain inadequate mentorship expose students to cyber threats (Hair et al., 2014; Kuhail et

al., 2023; Ong et al., 2024). Numerous users perceive themselves as protected through antivirus applications; however, spyware and viruses continue to present substantial risks, and although users do not bear sole responsibility for their security, they must implement protective measures (Furnell, 2008). In India, the government has implemented interventions through the Nirbhaya Fund, which facilitates cyber awareness and safety services for students, in conjunction with the National cybercrime Reporting Portal and awareness initiatives that enable women to identify and report online threats, Supplementary mechanisms include One Stop Centers, ERSS-112, Women Help Desks, the Women Helpline, expedited judicial Proceedings, Anti-Human trafficking Units, and the Central Victim Compensation Fund (PIB, 2025).

Objectives

- To assess college students' awareness of social media usage and online harassment in Coimbatore city.
- To analyze the association of age and educational qualification with students' awareness of social media and content sharing
- To identify the key dimensions of students' awareness of cyber safety initiatives and reporting mechanisms.
- To examine students' satisfaction with the protection available under cybersecurity laws.

2

2. Materials and Methods

Cybersecurity has emerged as a critical concern in the digital age, primarily due to the increased risks associated with online activities. According to Geetanjali (2020) examined that approximately 10 million users are at risk of being stalked, robbed, harassed, or worse. Similarly, the Centre for strategic and International Studies (CISS) reported an annual financial loss of 445 billion dollars to the global economy as a result of cybercrime.

Simon and Mary (2023) emphasize the women's perceptions regarding cybersecurity awareness by comparing the awareness levels among homemakers, working women, and students, as well as identifying preventive measures of cyber threats. In the contemporary digital environment, characterized by the rapid expansion of online activities, the study focuses on the awareness levels and fundamental knowledge of cybersecurity among female college students in Coimbatore city. It indicates a persistent deficiency in practical knowledge regarding the implementation of essential security measures for safe and secure network usage.

Krutika Bhate (2023) analyzed that the students were aware about password security and social media security whereas they have less awareness about browser security. The awareness session found effective in generating awareness about cybercrime and cyber security among the female university students. Less number of students attended the session; they should understand the importance of cyber security. The study concludes that there is a great need of generating awareness about cyber security among the students. The findings of the study recommend that universities should include curriculum on cyber security for the students.

Vimal Pandya (2024) examined the nature of cyber threats targeting women, the socio psychological impact of these threats, and the existing measures to counter them. The study further provides actionable recommendations to enhance cybersecurity awareness, policy interventions, and technological solutions tailored for women's safety online. By presenting detailed findings and recommendations, the paper aims to contribute to the creation of a safer and more equitable digital environment for women globally.

According to Netshlunda and Madzvamuse (2025), emphasizes the connection between cybersecurity awareness and strategic initiatives within rural university settings. It underscores the significance of awareness programs, digital literacy, and effective governance policies in enhancing cybersecurity within these institutions. There is a pressing need for structured educational programs that empower students to utilize digital tools in a safe, secure, and productive manner, thereby bolstering support for teachers' professional development. Consequently, essential elements such as critical thinking, information verification, and creative problem-solving should be integrated into educational reforms to enhance students' digital literacy and cybersecurity competencies (Hasan Tasay 2025).

Suzanne et al (2026) examines the beneficial correlation between data protection awareness, psychological factors, and the implementation of protective strategies, including social media, email, and cloud storage. They aim to identify deficiencies in teachers' awareness of cyber-attacks, a limited grasp of media literacy concepts, and the integration of training into teacher education programs. Additionally, they advocate for professional development opportunities for educators at all educational levels.

This investigation employed a quantitative methodological framework utilizing primary data obtained from 111 college students across designated regions of Coimbatore city. The research utilized a convenience sampling approach, with data collection facilitated through Google Forms. The survey instrument encompassed inquiries regarding participants' sociodemographic characteristics, patterns of social media engagements, awareness of cyber safety protocols, and perceived adequacy of legal protections under cybersecurity legislation. The acquired data underwent analysis employing frequency distributions, percentage calculations, Chi-square testing, one-way analysis of variance (ANOVA), Factor Analysis, and Structural Equation Modelling (SEM). These analytical techniques were implemented to examine associations among variables, quantify cyber safety awareness levels, and evaluate students' perceptions regarding the effectiveness of cybersecurity legal protections.

3

3. Results

The current research involves the analysis and interpretation of data gathered from a sample survey conducted among college students, utilizing a google form, as presented below:

Socio-Demographic Profile of the respondents:

The survey instrument encompassed several distinct sections addressing participant demographics, patterns of social media engagement, apprehensions regarding privacy, tendencies towards excessive information disclosure, and protective measures including the implementation of robust passwords and two-factor authentication protocols. This population was chosen because university students constitute one of the most engaged user segments across social media platforms and consequently face heightened exposure to privacy vulnerabilities and potential data compromise. The questionnaire was administered via digital platforms and institutional communication systems to ensure representation from a heterogeneous participants population (Sahu et al., 2026). This section deals the Socio-Demographic profile of the respondents includes variables such as age, educational qualifications, marital status, family type, and monthly family income, which have been analyzed in the table below (Table 1).

Characters	Characteristics	Frequency	Percentage (%)
Age (in Yrs)	17-26	94	84.7
	27-36	15	13.5
	37-46	2	1.8
Education Qualification	UG	78	70.3
	PG	17	15.3
	PhD	16	14.4
Marital Status	Married	9	8.1
	Unmarried	102	91.9
Type of Family	Joint Family	25	22.5
	Nuclear family	76	68.5
	Single Parent Family	10	9.0
Family Monthly Income (in Rs.)	10000-20000	34	30.6
	21000-30000	16	14.4
	31000-40000	9	8.1
	41000-50000	10	9.0
	51000-above	41	36.9
	Nil	1	0.90
	Total	111	100

Table 1: Socio-Demographic Profile of the respondents. Source: Filed Survey, 2026

Table 1 illustrates that 94 percent of the respondents fall within the age range of 17-26 years, representing the highest percentage among all age groups. Conversely, the age group of 37-46 years has the lowest representation at 2%. In present study, most respondents completed Under Graduation (78%), followed by Post Graduation (17%), while only (16 %) each completed PhD, which is important for any socio-

demographic study, majority of them were Unmarried (102%) and (9%) of respondents were married. This indicates the total number of members in the family which is majority of people belonging to the nuclear family (76%) and the least number of respondents in the survey were belongs to Single Parent Family (10%). The highest proportions of respondents (41%) belong to the Rs.51000 and above income group, while the lowest proportion (1%) respondents no family income. Overall, the socio-demographic profile shows that the study mainly represents young and educated respondents who are active users of digital platforms and therefore more relevant to understanding cybercrime awareness and online safety.

Chi-Square Analysis

According to studies, many students are not sufficiently aware of the threats and safety precautions related to online security, even if cybercrimes are becoming more common. Students who lack cybersecurity awareness are not only at risk, but it may also have wider repercussions when they grow up to be professionals in charge of protecting digital infrastructures and handling sensitive data (Pooja & Riddhi 2025). In order to investigate the relationship between Awareness on social media and age (Time spent on social media, use of social media platforms, Frequent users of social media platforms, Forms of online harassment, Platforms with Abusive content) of the respondent's chi-square test was done. The null hypothesis framed was:

H₀: There is no significant association between Awareness on social media and age

H_a: There is a significant association between Awareness of social media and age

The calculated chi-square values are shown in table 2.

Variables	Chi-square	Df	Sig.	Inference
Age	134.000	2	.000	Reject Ho
Time Spent on social media	50.622	3	.000	Reject Ho
Use of social media platforms	84.766	1	.000	Reject Ho
Frequent users of social media platforms	96.324	8	.000	Reject Ho
Forms of Online Harassment	26.541	6	.000	Reject Ho
Platforms with Abusive content	105.378	5	.000	Reject Ho

Table 2: Relationship between Awareness on social media and Age among college students. Source: Primary data, 2026

The present study found a statistically significant association at the 1% level ($P < 0.01$) between age and awareness of social media, including Time spent on social media, use of social media platforms, types of platforms used, forms of online harassment, and platforms containing abusive content. This concludes that age influences the level of social media awareness among college students.

ANOVA TEST

The impact of a digital citizenship education program on the cyber-safety knowledge and behavior of college students. The study found that after participating in the program, students had significantly increased their knowledge of cyber-safety and were more likely to engage in safe digital practices, such as using strong passwords and avoiding clicking on suspicious links Adorjan and Ricciardelli (2019). A quantitative analysis was carried out to find whether there is any significant difference between educational qualification and the usage of Internet. The null hypothesis tested was,

H₀: There is no significant association between the usage of Internet browsers and educational qualifications among college students.

H_a: There is significant association between the use of an Internet browser and Educational Qualification among college students. The calculated ANOVA values are shown in Table 3.

Variables		Sum of squares	df	Mean squares	F	Sig.	Inference
Most Used Internet Browser	Between Groups	9.593	3	3.198	2.164	.097	Not Significant
	Within Groups	158.137	107	1.478			
	Total	167.730	110				
Main purpose of Internet	Between Groups	3.300	3	1.100	1.077	.362	Not

Use	Within Groups	109.259	107	1.021			Significant
	Total	112.559	110				
Content sharing on social media	Between Groups	.275	3	.092	.357	.784	Not Significant
	Within Groups	27.472	107	.257			
	Total	27.748	110				
Type of content shared on social media	Between Groups	40.817	3	13.606	4.733	.004**	Significant
	Within Groups	307.579	107	2.875			
	Total	348.396	110				
Common Suspicious Content on social media	Between Groups	18.697	3	6.232	3.041	.032**	Significant
	Within Groups	219.267	107	2.049			
	Total	237.964	110				
Response to Suspicious Content	Between Groups	2.756	3	.919	.608	.611	Not Significant
	Within Groups	161.640	107	1.511			
	Total	164.396	110				

Table 3: Test Influence of Educational Qualification with various factor tested through one way ANOVA.

Source: Based on Author's Calculation

**** -Significant at 5% level, * -Significant at 10% level**

The table presented above found that there is no statistically significant difference between and within the groups at the 5% level ($p > 0.05$) with respect to the impact of educational qualification on various factors which is Most used Internet Browser, Main purpose of Internet Use, Content sharing on social media, Response to suspicious Content. However, a statistically significant difference at the 5% level ($p < 0.05$) was observed among the selected groups which is Type of content shared on social media and Common suspicious content on social media. The survey concludes that educational qualification has a significantly influences on the content shared and the suspicious content found on social media platforms.

Awareness about Cyber Safety

Cybercrime awareness refers to a person's knowledge of the nature of cyber offences, the techniques used by offenders, the laws against such acts, and the precautions one can take while operating in cyberspace (Alqahtani, 2022). Factor analysis was used in the present study to identify awareness about cyber safety of the college students and whether this awareness can be grouped in terms of a composite variable. To determine the appropriateness of applying factor analysis the KMO and Bartlett's test measures were computed and the results are presented in the table 4.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.853
Bartlett's Test of Sphericity	Approx. Chi-Square	1559.955
	Df	190
	Sig.	.000

Table 4: KMO and Bartlett's Test. Source: Estimation based on field survey, 2026

The KMO statistics for Awareness about Cyber safety of college students were recorded at 0.853, signifying higher than acceptable level of sampling adequacy. All the variables had values greater than 0.50 signifying substantial portion of the variance accounted by the factors. The table 5 presents the Eigen values, there relative explanatory powers and factor loadings for 16 linear components identified within the data set.

Awareness about Cyber Safety	Component			
	1	2	3	4
I am aware of Cyber safety posters, ads, or TV campaigns by the government.	.772			
I know about the National Cyber Crime Reporting Portal	.727			

I am aware of the Kavalan SOS App launched by Tamil Nadu Police for women's Safety.	.715			
I am aware of RBI campaigns on UPI frauds and safe digital payments.	.696			
I know that strong passwords and two-factor authentication are promoted in government campaigns.	.677			
I am aware that cyber-crime cells exist in every state for women's safety.		.764		
I am aware that police and government encourage women to report online harassment without fear.		.710		
More local language campaigns are needed to reach rural women		.657		
I know that awareness programs focusing on safe use of online banking and UPI.		.640		
Government's cyber Surakshit Bharat initiative is useful for spreading cyber safety awareness.			.799	
I know about the Digital Shakti campaign for women's online safety.			.765	
I am aware that CERT- In (Indian Computer Emergency Response Team) gives cyber alerts and guidelines.			.765	
Government campaigns have improved women's awareness about safe use of social media			.656	
Government conducts awareness drives in schools/colleges on cyber safety.			.649	
I am aware of the Cyber Swachhta Kendra (Government botnet cleaning and antivirus initiative).				.720
I am aware that free antivirus tools are recommended by government portals.				.605
Eigen value	9.701	1.772	1.270	1.011
Percentage of Variance explained	48.507	8.859	6.349	5.057
Total variance explained	48.507	57.366	63.716	68.773

Table 5: Rotated Component Matrix

Extraction Method: Principal Component Analysis Rotation Method: Varimax with Kaiser Normalization. A rotation converged in 16 interactions

The findings suggest that for the sample, the Eigenvalue for each factor must exceed one, signifying that these factors are suitable for inclusion in the factor analysis. Collectively, these factors represented approximately 69 percent of the variation in the factor. Factor 1 has Significant loading on Five dimensions namely 'I am aware of Cyber safety posters, ads, or TV campaigns by the government', 'I know about the National Cyber Crime Reporting Portal', 'I am aware of the Kavalan SOS App launched by Tamil Nadu Police for women's Safety', 'I am aware of RBI campaigns on UPI frauds and safe digital payments', 'I know that strong passwords and two-factor authentication are promoted in government campaigns. These dimensions explained 49 percent of the variance. Factor 2 had significant loading on four dimensions namely 'I am aware that cyber-crime cells exist in every state for women's safety', 'I am aware that police and government encourage women to report online harassment without fear', 'More local language campaigns are needed to reach rural women', 'I know that awareness programs focusing on safe use of online banking and UPI'. These dimensions explained 9 percent of the variance. Factor 3 had significant loading on 5 dimensions namely 'Government's cyber Surakshit Bharat initiative is useful for spreading cyber safety awareness', 'I know about the Digital Shakti campaign for women's online safety', 'I am aware that CERT-In (Indian Computer Emergency Response Team) gives cyber alerts and guidelines', 'Government campaigns have improved women's awareness about safe use of social media', 'Government conducts awareness drives in schools/colleges on cyber safety'. These explained nearly 6 percent of the variance. Factor 4 had significant loading on 2 dimensions namely 'I am aware of the Cyber Swachhta Kendra (Government botnet cleaning and antivirus initiative)', 'I am aware that free antivirus tools are recommended by government portals. These dimensions explained 5 percent of the variance. To sum up overall cyber safety awareness is high because of effective government campaigns. However, there is a need to improve deeper understanding and practical knowledge of cyber safety tools. Strengthening local language outreach, institutional programs, reporting awareness, and use of preventive tools will help improve women's online safety and confidence.

Satisfaction among students with Protection under Cybersecurity Laws

The digital safety awareness implies women's awareness and understanding of protective measures to ensure their safety in the digital environments. The cybercrime awareness is tightly linked to the recognition of

risky online behaviors and preventive measures implementation (Ahmead, Sharif & Abuiram, 2024). The implications arising from the results are that digital safety awareness be more practical than cyber harassment exposure. This section deals with the satisfaction among students with protection under cybersecurity laws.

Fit Index	Obtained Value	Recommended value	Interpretation
χ^2	347	-	
Df	265	-	
CFI	0.997	≥ 0.90	Excellent fit
TLI	0.997	≥ 0.90	Excellent fit
NNFI	0.997	≥ 0.90	Excellent fit
RNI	0.997	≥ 0.90	Excellent fit
NFI	0.988	≥ 0.90	Excellent fit
IFI	0.997	≥ 0.90	Excellent fit
PNFI	0.872	≥ 0.50	Satisfactory fit
SRMR	0.061	≤ 0.08	Good fit
RMSEA	0.053	≤ 0.08	Good fit

Table 6: Model fit indices

The model demonstrates an excellent overall fit, as the incremental fit indices exceeds 0.90, while RMSEA and SRMR remain within commonly accepted limits. The X^2/df ratio of 1.31 also indicates good fit. Therefore, the model can be considered to have a good overall fit with the observed data. Taken together, the results suggest that the revised model provides an acceptable representation of the data and is suitable for subsequent structural analysis. Kaiser-Meyer-Olkin Measure is 0.903, given that acceptable sampling adequacy for running the model. The measurement model exhibited generally satisfactory convergent validity, with all standardized factor loadings exceeding the recommended threshold of 0.50. Strong loadings were observed across the constructs, with loadings ranging from 0.614 to 0.870. Unlike previous model configurations, the finalized constructs – Legal resources (LR), Awareness and reporting (AR), Risk Factors (RF), Safety measures (SM), and Effectiveness of Intermediaries (EI) did not display comparatively weaker indicators, as even the lowest loading. Overall, the findings support the adequacy of the measurement model and justify proceeding with structural model estimation and hypothesis testing.

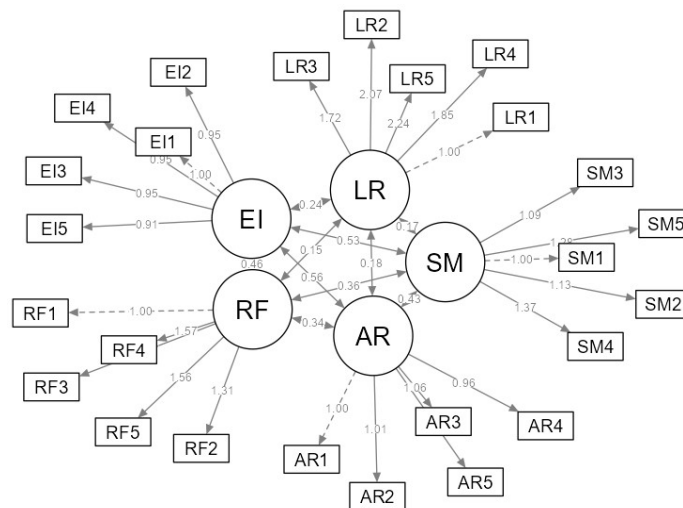


Figure 1

The SEM analysis on Satisfaction of Protection for Women under Cyber Security Laws indicates that the respondents have a moderate level of satisfaction with the existing cybersecurity protection mechanisms. The findings suggest that students perceive the available laws, protection mechanisms, and institutional measures as providing a certain level of safety and helping to reduce cyber risks. However, their satisfaction is not high, mainly due to limited awareness of legal provisions, difficulties in the procedures for seeking protection or reporting cyber incidents, and inadequate support mechanisms.

Therefore, the overall SEM finding indicates that respondents are moderately satisfied with the protection available for women under cybersecurity laws, but there is still a considerable gap between the availability of protection mechanisms and their effective awareness and utilization. Strengthening awareness of cyber laws, simplifying reporting procedures, and improving institutional support could enhance students' satisfaction with cybersecurity protection mechanisms.

4. Discussion

The study found that young and educated respondents are active users of digital platforms and are generally aware of online safety practices. College students were moderately aware of social media platforms, including time spent, platforms used, forms of online harassment and platforms containing abusive content, and age was significantly associated with this awareness. Most of undergraduate and postgraduate students were not fully aware, therefore it requires digital literacy and awareness programmes. Students also need practical knowledge of cyber safety tools and reporting mechanisms, which would improve women's online safety and confidence. Strengthening cybersecurity laws, reporting procedures and institutional support would further enhance students' satisfaction with protecting mechanisms. Future research may extend this work to larger and more diverse samples and examine the effectiveness of awareness interventions.

5. Conclusion

The study concludes that students need to improve their digital literacy and awareness of social media and cyber safety practices so that they can use digital platforms safely and confidently. College students were generally having awareness of online safety practices but only few are moderately aware of social media use. Awareness programmes should focus on cybersecurity and the safe use of online banking and UPI, with local-language campaigns to reach rural women. The government and police should encourage women to report online harassment without fear, and students should be encouraged to use women's safety apps such as the Tamil Nadu Police's Kavalan SOS app. Strengthening cyber laws and protection mechanisms would further enhance students' satisfaction.

References

- Adorjan, M.; Ricciardelli, R. (2019) Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learn. Media Technol.* 44, 430–442.
- Ahamed, B., Polas, M. R. H., Kabir, A. I., Soheli-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. *Sage Open*, 14(1), 21582440241228920.
- Ahmed, M., El Sharif, N., & Aburam, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at the Al Quds University: A cross-sectional study. *Crime Science*, 13, Article 29.
- Alqahtani, M. A (2022) Factors Affecting Cybersecurity Awareness among University Students *Journal of Applied Science* Volume 12 Issue 05, 2589;
- Chelsea Angelina Simon & Sagaya Anglien Mary (2023) Awareness on Cyber Security among students in women colleges with special reference to Coimbatore city *International Journal of creative research thoughts (IJCRT)* 11(4): 2320-2882.
- F. Hair Jr J, Sarstedt M, Hopkins L, G. Kuppelwieser V (2014), "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research". *European Business Review*, 26 (2) 106 – 121.
- Geetanjali & Gulnaz (2020) Women perception towards awareness and preemptive measures of cyber security: A study *Journal of Interdisciplinary Cycle research* XII (X): 0022 – 1945.
- Hollynness Netshlunda & Madzvamuse (2025) A Systematic Literature Review of Cybersecurity Awareness and Strategy in Rural-Based Universities *International Journal of Applied Research in Business and Management* 6 (5): 2700-8983
- Kim, E. B. (2013). Information security awareness status of business college: A global perspective of undergraduate students. *Information Security Journal*, 22(4), 171-179. ISSN: 1939-3547
- Krutika Bhate (2023). A Study on Awareness about Cyber Security Among the Female University Students. *International Journal on Emerging Technologies*, 14(2): 13–19: 2249-3255
- Kuhail, M. A., Alturki, N., Alramlawi, S., & Alhejori, K. (2023). Interacting with educational chatbots: A systematic review. *Education and Information Technologies*, 28(1), 973-1018

Kuhail, M. A., Alturki, N., Alramlawi, S., & Alhejori, K. (2023). Interacting with educational chatbots: A systematic review. *Education and Information Technologies*, 28(1), 973-1018.

Moallem A. (2018) Cyber security awareness among college students *Advances in intelligent systems and computing Springer International Publishing*; 2019. 79–87: 978-3-319-94781-5

Moallem, A. (2017). Do you really trust “privacy policy” or “terms of use” agreements without reading them? In *Advances in Human Factors in Cybersecurity* (pp. 290-295). Springer.

Mohd Zubair (2026) A Study of Awareness on Cybercrime among Students of Constituent Colleges of Cluster University Jammu *International Journal of Research and Innovation in Applied Science (IJRIAS)* Volume XI Issue I ISSN No: 2454-6194

Mohd Zubair (2026) A Study of Awareness on Cybercrime among Students of Constituent Colleges of Cluster University Jammu *International Journal of Research and Innovation in Applied Science (IJRIAS)* Volume XI Issue I ISSN No: 2454-6194

Nilupú-Moreno, K., Salas-Riega, J.L., Ninaquispe-Soto, M., Riega-Virú, Y. (2024). Cybersecurity in University Students: A Systematic Review of the Literature. In: Nagar, A.K., Jat, D.S., Mishra, D.K., Joshi, A. (eds) *Intelligent Sustainable Systems*. WorldS4 2023. Lecture Notes in Networks and Systems, vol 817. Springer, Singapore.

Ong, M. F., Soh, K. L., Saimon, R., Saidi, H. I., Tiong, I. K., Myint, W. W., ... & Japar, S. (2024). Predictors of fall protection motivation among older adults in rural communities in a middle-income country: A cross-sectional study using the Protection Motivation Theory. *Journal of Advanced Nursing*, 80(12), 4946-4962.

PIB (2025) Curbing Cyber Frauds in Digital India.

Pooja & Riddhi (2025) Cyber security Awareness: Social Media Usage and Cyber Security Behavior of College students *International Journal of Advance and Applied Research (IJAAR)* Vol 6 Issue no.16 ISSN: 2347-7075

Sahu. L. R., Kumar. V., Nair. R. S., Karkera. A (2026) Social media privacy & Data Leaks: Risks, User Behaviour, and Cybersecurity Awareness among students 13(05) 101-106 ISSN: 2395-0072

Steven Furnell (2008) End-User security culture: A lesson that will never be learnt? *Computer Fraud & Security* Volume 2008, Issue 4 PP 6-9

Suzanne Lok Tung, Wing Ho, & Warren Ka Chun Tam (2026) Professional Development in Enhancing Teachers' Cybersecurity Awareness: Current Status and Future Directions of Media Literacy Training Education Science 16(2)

Tasay, H., & Demir Basaran, S. (2025) An Analysis of K12 Students' Digital Literacy and Cybersecurity Awareness in the Context of Teachers' Views. *Cypriot Journal of Educational Sciences*, 20(2), 127–136.

Vimal Pandya (2024) Cyber Security for Women: A Comprehensive Study of Threats, Challenges, and Solution *International Journal of Novel Research and Development (IJNRD)* Volume 9, Issue 12 ISSN: 2456-4184

Conflicts of Interest: The authors declare “No conflict of interest”.

AUTHORS' BIO-NOTES

Priyanka J is a PhD Research Scholar in Economics at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. She completed her undergraduate degree at PSGR Krishnammal College for Women and her postgraduate degree at Avinashilingam Institute for Home Science and Higher Education for Women, and now pursuing doctoral research in Economics, specializing in cybercrime and digital financial fraud. She has presented research papers at national and international seminars and conferences, including the National Seminar on “Women Empowerment for Health and Sustainability: A Pathway to Global Well-being” at Avinashilingam Institute and the International Seminar on “Sustainable Development Goals in India: Achievements and Challenges Ahead” at Gandhigram Rural Institute. Priyanka also attended an ICSSR-SRC-sponsored national seminar on sustainable growth, fintech, MSMEs, and green strategies. Her conference papers have published in ISBN-indexed proceedings.

Dr. Malarvizhi V joined Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, as Lecturer in Economics in 2004 and became Professor and Head of Economics in 2020. With 20 years of teaching experience at UG and PG levels, she specializes in Banking, Gender Studies, and Development Economics. She completed an ICSSR-sponsored major research project of Rs. 22 lakh and evaluated a UGC Major Research Project.

Dr. Malarvizhi guided 24 PG scholars, two M.Phil. scholars, and currently guiding four PhD scholars. She has 73 publications, including 41 international journal articles, 12 national journal articles, six conference proceedings, and 14 book chapters. She edited three books, authored two books, and edited special issues for four journals. She received Excellent and Best Paper Awards, presented papers at 31 conferences, organized five conferences and one FDP, and contributed to E-PG Pathshala. She is an NCC Officer and received DG NCC Medallion Award in 2019.