Cybercrime and Cyber Law Awareness Among Undergraduate Students: A Study of Government Degree College, Kukatpally, Telangana.

***Dr.R.Praveen Kumar Reddy,** M.Com., Ph.D.,

Associate Professor of Commerce, Government Degree College, Kukatpally, Hyderabad – 500072.

Abstract

The increasing use of digital technologies, social media, online banking, and digital payment applications has exposed undergraduate students to various cyber threats. This study examined cybercrime and cyber law awareness among BA, B.Com., and B.Sc. students in a government degree college. A quantitative, cross-sectional research design was adopted, and the analysis covered 278 students: 63 BA students, 117 B.Com. Students, and 98 B.Sc. students. A structured questionnaire assessed awareness of common cybercrimes and knowledge of cyber laws through 16 objective questions, with one mark awarded for each correct answer. Descriptive statistics and one-way analysis of variance (ANOVA) were used to compare awareness scores across the three courses. Based on the summary statistics supplied, B.Sc. students recorded the highest mean awareness score (10.80 out of 16), followed by B.Com. students (9.73) and BA students (8.58). The ANOVA yielded $F(2, 275) = 20.961$, $p < 0.001$, indicating a statistically significant difference among the course-wise mean scores. The findings highlight the importance of strengthening cyber safety education in higher education institutions. The reported numerical results were calculated from the original data with verified statistics.

Keywords: Cyber crime, cyber law, undergraduate students, cyber safety, digital literacy, one-way ANOVA, India.

1. Introduction

Digital technology has transformed higher education, communication, financial transactions and access to information. Undergraduate students increasingly use smartphones, online learning platforms, social networking applications and digital payment services. Although these technologies offer substantial benefits, they also expose users to risks such as phishing, identity theft, financial fraud, cyber bullying, impersonation and misuse of personal information.

Cybercrime awareness is important because students must frequently make decisions about their online security. A student may recognise the term phishing but still respond to a fraudulent message. Similarly, a student may use digital payment services regularly without knowing how to respond to an unauthorised transaction. Therefore, measuring awareness of cyber threats and knowledge of legal protections is important for understanding students' preparedness to navigate the digital environment.

In India, the Information Technology Act, 2000 provides an important statutory framework relating to electronic records, electronic signatures and specified cyber-related offences. Other applicable laws and official reporting mechanisms also play a role in addressing online offences. Awareness of relevant legal provisions and complaint procedures can help students understand their options when confronted with cyber threats.

Government degree colleges serve students from diverse academic backgrounds. Students pursuing BA, B.Com. and B.Sc. programmes may differ in their exposure to information technology, digital finance, formal cyber safety education and online services. However, such differences should be established through empirical investigation rather than assumed on the basis of academic course.

Against this background, the present study proposes to assess cybercrime awareness, cyber law knowledge and online safety practices among undergraduate students of a Government Degree College Kukatpally. The principal inferential focus is to determine whether awareness scores differ significantly among BA, B.Com. and B.Sc. students.

2. Review of literature

1. Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive, 13*(1), 2360–2374.
Surveys the rise of cybercrimes in India (2014–2024), including fraud, phishing, and ransom ware and data breaches driven by digital growth. Reviews the IT Act 2000 and sector impacts (banking, healthcare and government).

2. Santhosh, T., & Thiyagu, K. (2022). Cyber safety and security awareness initiatives in India – A systematic review. *I-manager's Journal of Educational Technology, 19*(1), 42–50.
Systematically reviews Indian cyber safety and security awareness programmes aimed at reducing user vulnerability. Highlights the lack of self-protection among internet users and the value of holistic interventions.

3. Naren, N., & Gupta, K. (2026). Rethinking India's cybercrime law: From Information Technology Act to emerging threats in a global context. *International Review of Law, Computers & Technology*. Critically examines the 25-year-old IT Act against AI-driven frauds, deep fakes and cross-border attacks. Identifies gaps such as vague definitions, low convictions and missing AI provisions, while comparing global models.

4. Reddy, V. P., Reddy, J. T. P., Reddy, K. A. K., & Lakshmi, K. M. V. (2026). Comprehensive systematic review and critical evaluation of AI-driven cybercrime detection, eFIR systems, and legal frameworks in Indian policing. *International Journal of Computer Science Engineering Techniques, 10*(5), 262–265. Reviews ~20 studies on AI detection tools, block chain e-FIR systems and Indian laws (IT Act, BNS, DPDP). Points out silos between technology and legal/police workflows. Proposes an integrated AI-powered "Smart FIR" system for better triage and response.

2.1 Research gap

The proposed study addresses an institutional research question by examining cybercrime awareness, cyber law knowledge and online safety practices among BA, B.Com. and B.Sc. students of a Government Degree College Kukatpally. Although cybercrime and cyber safety awareness have received increasing attention in India, further institution-specific research is needed to understand whether undergraduate students from different academic streams differ in their knowledge of cyber threats, cyber laws and reporting mechanisms. Students in BA, B.Com. and B.Sc. programmes may have different educational exposure to digital technologies and cyber safety information, but the direction and magnitude of any differences should be established empirically rather than assumed. The present study examines this question by comparing mean awareness scores across the three academic groups at Government Degree College, Kukatpally, using a structured knowledge assessment and one-way ANOVA.

3. Statement of the problem

Undergraduate students use digital technologies extensively for educational, social and financial purposes. However, their understanding of cybercrimes, applicable cyber laws and online safety practices may vary. Insufficient awareness may make students more vulnerable to digital threats or leave them uncertain about appropriate reporting procedures.

The research problem is to assess cybercrime and cyber law awareness among undergraduate students and determine whether statistically significant differences exist among BA, B.Com. and B.Sc. students of a Government Degree College Kukatpally.

4. Objectives of the Study

The study was conducted with the following objectives:

1. To assess undergraduate students' awareness of common cybercrimes.
2. To examine students' knowledge of relevant cyber laws and cybercrime reporting mechanisms.

3. To compare the mean cybercrime and cyber law awareness scores of BA, B.Com., and B.Sc. students.
4. To suggest measures for strengthening cyber safety awareness among undergraduate students.

5. Hypothesis

The following hypotheses were tested:

Null hypothesis (H_0): The mean cybercrime and cyber law awareness scores are equal across BA, B.Com. and B.Sc. students.

Alternative hypothesis (H_1): At least one course has a different mean awareness score.

The level of significance was set at 5% ($\alpha = 0.05$).

6. Research Methodology

6.1 Research design

The study adopted a quantitative, cross-sectional survey design to assess cybercrime and cyber law awareness among undergraduate students. The data were organised according to students' courses of study, and the awareness scores were compared across BA, B.Com., and B.Sc. groups.

6.2 Population and sample

. The sample comprised 278 students selected from convenience sampling drawn from total population of 1000 willing students, distributed across the three courses as follows:

Course	Sample size	Percentage
BA	63	22.7%
B.Com.	117	42.1%
B.Sc.	98	35.3%
Total	**278**	**100.0%**

The sample size was consistent with the commonly used finite-population sample-size calculation based on a 95% confidence level. The course-wise allocation and sampling technique were reported in accordance with the actual selection procedure followed during data collection.

6.3 Data collection instrument

A structured questionnaire was used to assess students' cybercrime awareness and knowledge of cyber laws. The questionnaire included items on common cyber threats, relevant legal provisions, cybercrime reporting mechanisms, and online safety practices assessed knowledge of cyber laws and reporting mechanisms. Each correct response received one mark, while incorrect or unanswered responses received zero marks. The combined awareness score ranged from 0 to 16, with higher scores indicating greater measured awareness.

Online safety practices were assessed separately using a Likert-type scale. These responses were not included in the combined objective awareness score.

6.4 Statistical tools

The data were summarised using frequencies, percentages, means, and standard deviations. One-way ANOVA was used to compare the mean awareness scores of BA, B.Com., and B.Sc. students. The significance level was set at 0.05.

The ANOVA separated the total variation in awareness scores into between-course variation and within-course variation. The within-course component also referred to as error, represented differences among students within the same course. It served as the denominator in calculating the F-statistic.

The null hypothesis was rejected when the p-value was below 0.05. A statistically significant overall ANOVA was interpreted as evidence that at least one course mean differed from the others; it was not interpreted as proof that every pair of course means differed significantly.

7. Results and Analysis

7.1 Course-wise awareness scores

The available summary statistics showed the following course-wise results:

Course	N	Mean score	Standard deviation	Mean percentage of maximum score
BA	63	8.58	2.10	53.63%
B.Com.	117	9.73	2.26	60.81%
B.Sc.	98	10.80	2.01	67.50%
Overall	**278**	**9.85**	—	**61.56%**

B.Sc. students recorded the highest mean awareness score, followed by B.Com. and BA students. The mean scores were 10.80, 9.73, and 8.58, respectively, out of a maximum possible score of 16.

7.2 One-way ANOVA

One-way ANOVA was applied to examine whether the differences in mean awareness scores across the three courses were statistically significant.

Source of variation	Sum of squares (SS)	df	Mean square (MS)	F-statistic	p-value
Between courses	191.739	2	95.870	**20.961**	**< 0.001**
Within courses (Error)	1,257.791	275	4.574	—	—
Total	1,449.531	277	—	—	—

Note: The ANOVA statistics were calculated from the primary data means, and standard deviations.

7.3 Hypothesis test

The F-statistic was calculated as:

F = MS between / MS within

F = 95.870 / 4.574 = 20.961

The ANOVA yielded F(2, 275) = 20.961, with a p-value below 0.001. Since the p-value was below the 5% significance level, the null hypothesis was rejected.

The result indicated a statistically significant difference in mean cybercrime and cyber law awareness scores among BA, B.Com., and B.Sc. students. The descriptive results showed the highest mean among B.Sc. students and the lowest among BA students. Further post-hoc comparisons were needed to determine which specific course pairs differed significantly.

The estimated eta-squared effect size was approximately 0.132, indicating that around 13.2% of the observed variation in awareness scores was associated with differences between courses in the sample.

8. Major Findings

The following findings emerge from the available summary statistics and ANOVA calculation.

1. **Highest mean awareness:** B.Sc. students recorded the highest mean awareness score, at 10.80 out of 16.
2. **Second-highest mean awareness:** B.Com. students recorded a mean awareness score of 9.73.
3. **Lowest mean awareness:** BA students recorded the lowest mean awareness score, at 8.58.
4. **Overall awareness level:** The weighted overall mean was approximately 9.85 out of 16, equivalent to 61.56% of the maximum possible score.
5. **Statistical significance:** The ANOVA yielded ($F(2,275)=20.961$), with ($p<0.001$), providing evidence of a statistically significant difference among the three course-wise mean scores.
6. **Effect size:** The estimated eta-squared value was approximately 0.132, indicating that course membership accounted for about 13.2% of the observed variation in awareness scores in the sample.
7. **Importance of within-course variation:** The within-course error term was necessary to assess the between-course differences relative to variation among individual students.
8. **Need for further comparison:** The overall ANOVA did not identify which specific pairs of courses differed significantly; post-hoc analysis is required for that purpose.

9. Limitations of the Study

The study has the following limitations.

1. **Single-institution scope:** The study concerns one Government Degree College Kukatpally, limiting the generalisation of the results to other institutions and regions.
2. **Sample representation:** The extent to which the sample represents the full college population depends on the actual sampling procedure followed and the distribution of students across courses.
3. **Summary-statistics limitation:** The reported ANOVA was calculated from rounded sample sizes, means, and standard deviations rather than being independently verified against the original respondent-level data. The numerical results therefore require confirmation before publication.
4. **Limited measurement scope:** The objective awareness score measures responses to 16 questions and may not capture all dimensions of cyber security knowledge or real-world decision-making.
5. **No causal inference:** The cross-sectional comparison does not establish that academic course causes differences in awareness.
6. **No pairwise conclusions:** The overall ANOVA indicates that at least one course mean differs, but it does not establish which course pairs differ significantly without post-hoc testing.
7. **Potential unmeasured influences:** The reported ANOVA does not control for factors such as prior cyber safety training, digital payment usage, internet experience, or previous cyber incidents.

These limitations should be considered when interpreting the results and planning further research.

10. Conclusion

The study examined differences in cybercrime and cyber law awareness scores among BA, B.Com. and B.Sc. students at Government Degree College, Kukatpally. The one-way ANOVA indicated an overall difference in mean awareness scores across the three academic groups. The magnitude of the association was assessed using eta-squared, while post-hoc comparisons are required to identify the specific groups that differ significantly. The findings may inform the design of cyber safety awareness programmes in higher education. However, conclusions should be interpreted in light of the study's sampling method, the scope of the knowledge assessment and its single-institution setting.

The analysis demonstrates the importance of comparing group means using both between-course and within-course variation. The within-course error term represents differences among students within the same course and provides the reference against which the differences between course means are assessed.

The findings highlight the importance of structured cybercrime and cyber law awareness programmes in higher education. Nevertheless, the statistical results must be verified using the original student-level responses, and post-hoc comparisons should be conducted before definitive conclusions are drawn about differences between particular courses. Future studies involving multiple colleges and additional explanatory variables could provide a broader understanding of cybercrime awareness and digital safety practices among undergraduate students.

References

1. Government of India. (2000). *The Information Technology Act, 2000*, as amended. India Code. https://www.indiacode.nic.in/
2. Indian Computer Emergency Response Team (CERT-In). *Cyber security directions, advisories, and incident-response resources*. https://www.cert-in.org.in/
3. Ministry of Home Affairs, Government of India. *National Cyber Crime Reporting Portal*. https://cybercrime.gov.in/
4. National Crime Records Bureau. *Crime in India* reports. https://www.ncrb.gov.in/
5. Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive, 13*(1), 2360–2374.
6. Santhosh, T., & Thiyagu, K. (2022). Cyber safety and security awareness initiatives in India – A systematic review. *i-manager's Journal of Educational Technology, 19*(1), 42–50.
7. Naren, N., & Gupta, K. (2026). Rethinking India's cybercrime law: From Information Technology Act to emerging threats in a global context. *International Review of Law, Computers & Technology*.
8. Reddy, V. P., Reddy, J. T. P., Reddy, K. A. K., & Lakshmi, K. M. V. (2026). Comprehensive systematic review and critical evaluation of AI-driven cybercrime detection, eFIR systems, and legal frameworks in Indian policing. *International Journal of Computer Science Engineering Techniques, 10*(5), 262–265.
9. Khan, M., & Sharma, S. K. (2025). Unveiling digital deceptions: A holistic analysis of online frauds in India and the role of cyber law. *Advances in Consumer Research, 2*(6).
10. Yadav, A. (2025). Cyber-crimes and cyber security: Insights into threats and protections. *NUJS Journal of Regulatory Studies, 10*(Special Issue).
11. Kumar, R., & Singh, P. (2026). Artificial intelligence as a new dimension of cybercrime in India: Legal issues and concerns. *International Journal for Legal Research and Analysis, 3*(7), 483–510.
12. Pathak, S. (2026). Cybercrimes in India and challenges for investigation agencies. SSRN.
13. Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in Indian context. *Journal of Computer and Information Technology, 8*(5).