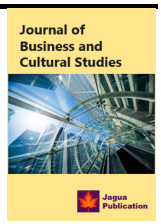
Jagua Publication

Journal of Business and Cultural Studies, 1(1):14–18, 2026. DOI: 10.58614/jbcs113

Journal of Business and Cultural Studies

Journal homepage: https://www.jpub.org/journal-details.php?journal-id=49



Case Study

Cybercrime Awareness and Digital Literacy among Undergraduate College Students: A Regional Empirical Study

T. Sakthiragavan[1]

[1]*Department of Business and Management, Govt Arts College, Chennai, Tamilnadu*
[*]*Corresponding author: sakthi34@gmail.com*

Article Info

Keywords: *Cybercrime, Digital Literacy, Cyber Awareness, Undergraduate Students*

Received: *01.06.2026;*
Accepted: *22.06.2026;*
Published: *28.06.2026*

Abstract

The rapid digitalization of higher education has increased students' exposure to cyber threats. This study investigates the level of awareness of cybercrime among undergraduate students. A total of 300 students were selected from Government Arts College, Thiruverumbur; Jamal Mohamed College; and Anna University College of Engineering, Trichy using stratified random sampling. Data were analyzed using percentage analysis, mean, standard deviation, independent sample t-test, ANOVA, and correlation analysis. The findings indicate moderate overall awareness, higher technical knowledge among engineering students, and significant gender and institutional differences. Legal literacy and reporting awareness remain comparatively low. The study recommends integrating cyber safety education into undergraduate curricula.

1. Introduction

The proliferation of internet access, smartphones, and digital transactions has significantly transformed academic and social life, bringing greater convenience and connectivity. However, this transformation has also expanded exposure to cyber threats such as phishing, identity theft, hacking, cyber bullying, and online banking fraud. India has witnessed a sharp rise in cybercrime cases in recent years, reflecting the growing risks associated with digital dependence. Undergraduate students, as active and frequent users of digital platforms for learning, communication, and social interaction, are particularly vulnerable to these threats. At the same time, they represent a crucial group for promoting cyber awareness and safe online practices. Despite the widespread use of digital technologies among students in this region, there is a noticeable lack of district-level empirical research focusing on cybercrime awareness. This gap limits the understanding of students' knowledge, attitudes, and practices related to cyber security. Therefore, there is a pressing need to examine the level of awareness and preparedness among undergraduate students in this district. This study aims to address this gap by exploring cybercrime awareness and identifying areas where educational interventions are required.

2. Review of Literature

Global research indicates that cybercrime awareness among youth varies significantly across regions and contexts. Riley and Manville [1] found that American university students were generally aware of common cyber threats such as phishing and malware. However, their understanding of legal remedies and reporting mechanisms remained limited. Similarly, Pokhrel and Chhetri [2] reported that Nepalese

students demonstrated moderate levels of cyber awareness. Despite this, they lacked adequate knowledge about formal reporting systems and procedures. These findings highlight a gap between technical awareness and institutional knowledge. Overall, global studies emphasize the need for comprehensive cyber education that includes both prevention and legal awareness. In the Indian context, several studies have examined cybercrime awareness among students. Sharma and Singh [3] observed that while students were familiar with various cyber threats, they lacked knowledge of legal provisions under the Information Technology Act (2000). Kumar and Rajan [4] identified a "cyber literacy gap" among students in Tamil Nadu. Their study showed that students possessed relatively higher technical knowledge but weak understanding of cyber laws. This imbalance limits their ability to respond effectively to cyber incidents. The findings suggest the need for integrating legal literacy into digital education. Overall, Indian research reflects a similar trend of partial awareness among youth. Gender-based studies on cyber awareness present mixed findings. Sangwan and Kumari (2019) reported that male students tend to have higher technical awareness of cyber threats. Bhardwaj and Sharma [5] supported this view but also noted that female students show greater concern for online privacy and safety. These differences highlight varying perceptions and priorities between genders. While males may engage more with technical aspects, females often demonstrate cautious online behavior. Such insights are important for designing targeted awareness programs. Overall, gender plays a significant role in shaping cyber awareness and attitudes. Research on cybercrime reporting behavior reveals a consistent pattern of underreporting. Lwin and Wing [6] found that many victims hesitate to report cyber incidents due to fear and lack of confidence in the system. Thomas and Varghese [7] further identified stigma and limited procedural knowledge as key barriers to reporting. Many individuals are unaware of how and where to report cybercrimes. This leads to a gap between victimization and official reporting statistics. Improving awareness of reporting mechanisms is therefore essential. Overall, studies highlight the importance of encouraging transparent and accessible reporting systems. Despite the availability of national and international research, district-level comparative studies remain limited. Tiruchirappalli, being a major educational hub, lacks sufficient empirical research on cybercrime awareness. Most existing studies focus on broader regional or national contexts. This creates a gap in understanding localized patterns of awareness and behavior. There is a need to examine how students in this district perceive and respond to cyber threats. Addressing this gap will contribute to more targeted policy and educational interventions. Therefore, this study aims to fill the existing empirical void in Tiruchirappalli.

2.1. Objectives of the Study

- To measure the level of cybercrime awareness among undergraduate students.
- To analyze gender differences in awareness.
- To examine institutional differences.
- To study awareness regarding cyber laws and reporting procedures.
- To identify the relationship between internet usage and cyber awareness.

2.2. Hypotheses

- **H01:** There is no significant difference between male and female students in cybercrime awareness.
- **H02:** There is no significant difference among colleges in cybercrime awareness.
- **H03:** There is no significant relationship between internet usage frequency and cybercrime awareness.

3. Research Methodology

Research Design

The study adopts a descriptive survey method to assess cybercrime awareness among undergraduate students.

Sample Size

A total of 300 undergraduate students are selected for the study.

Sampling Technique

Stratified random sampling is used to ensure equal and fair representation from each institution.

Area of Study

The research is conducted in three colleges located in Tiruchirappalli District.

- Government Arts College, Thiruverumbur: 100 students
- Jamal Mohamed College: 100 students
- Anna University College of Engineering, Trichy: 100 students

Data Collection Tool

structured questionnaire is used to gather primary data from respondents.

Scale Used

The questionnaire is designed based on a 5-point Likert scale to measure responses.

Percentage Analysis

Used to analyze and interpret the distribution of responses.

Mean and Standard Deviation

Applied to measure central tendency and variability in responses.

Independent Sample t-test

Used to compare differences between two groups.

One-way ANOVA

Applied to examine differences among multiple groups.

Pearson Correlation

Used to identify relationships between variables.

Percentage Analysis

Table 1: Gender Distribution

Gender	Frequency	Percentage
Male	160	53.3%
Female	140	46.7%

The gender distribution of the respondents shows that 53.3% are male and 46.7% are female. This indicates a slightly higher representation of male students in the study, though the sample remains fairly balanced, allowing for meaningful gender-based comparisons.

Table 2: Types of Cybercrime Distribution

Category	Frequency (%)	Percentage (%)
Phishing	72	28
Identity Theft	65	35
Cyber Bullying	78	22
Online Banking Fraud	81	19
Hacking	69	31

The data reveals varying levels of awareness among students regarding different types of cybercrime. Awareness is highest for online banking fraud (81%), followed by cyber bullying (78%). Phishing and hacking show moderate awareness levels, while identity theft has comparatively lower awareness at 65%. Overall, students are more familiar with commonly discussed or experienced cyber threats.

The overall mean score of 3.53 indicates a moderate level of cybercrime awareness among students. Higher mean values are observed for awareness of different cybercrimes and the use of strong passwords, suggesting better understanding of basic security practices. However, lower mean scores for awareness of cyber laws (3.12) and reporting procedures (3.20) highlight significant gaps in legal knowledge and formal response mechanisms. The standard deviation values indicate moderate variability in responses, suggesting differences in awareness levels among students.

Table 3: Awareness and Practices Related to Cybersecurity

Statement	Mean	Std. Deviation
Aware of different cybercrimes	3.84	0.92
Know how to protect accounts	3.67	1.01
Aware of cyber laws	3.12	1.18
Use strong passwords	3.75	0.98
Verify suspicious links	3.58	1.05
Know reporting procedure	3.20	1.14
Overall Mean Score	3.53	–
Overall Std. Deviation	–	1.05

Hypothesis Testing

Table 4: Gender-wise Comparison of Mean and Standard Deviation

Gender	Mean	Std. Deviation
Male	3.61	0.98
FeMale	3.44	1.07

t = 2.12, p = 0.035 (<0.05)

The independent sample *t*-test was conducted to examine whether there is a significant difference in cybercrime awareness between male and female students. The results indicate that male students (Mean = 3.61) have slightly higher awareness compared to female students (Mean = 3.44). Since the *p*-value (0.035) is less than 0.05, the null hypothesis H_0 is rejected. This suggests that there is a statistically significant difference in cybercrime awareness based on gender. The findings imply that gender plays a role in influencing awareness levels among students.

Table 5: College-wise Comparison of Mean and Standard Deviation

College	Mean	Std. Deviation
Govt Arts College	3.32	1.12
Jamal Mohamed College	3.47	1.04
Anna University	3.80	0.89

F = 6.45, p = 0.002 (<0.05)

A one-way ANOVA test was used to determine whether there are significant differences in cybercrime awareness among students from different colleges. The results show that Anna University students have the highest awareness level (Mean = 3.80), followed by Jamal Mohamed College (Mean = 3.47) and Government Arts College (Mean = 3.32). Since the *p*-value (0.002) is less than 0.05, the null hypothesis (H_0) is rejected. This indicates that there are statistically significant differences in awareness levels across institutions. The variation may be attributed to differences in academic exposure, curriculum, and access to digital resources.

Table 6: Correlation between Internet Usage and Awareness

Variables	r-value	p-value
Internet Usage & Awareness	0.42	< 0.01

Pearson correlation analysis was conducted to examine the relationship between internet usage and cybercrime awareness. The correlation coefficient ($\gamma = 0.42$) indicates a moderate positive relationship between the two variables. This means that as internet usage increases, cybercrime awareness also tends to improve. The *p*-value (< 0.01) confirms that the relationship is statistically significant, leading to the rejection of the null hypothesis (H_0). These findings suggest that greater exposure to digital platforms may enhance students' familiarity with cyber threats and related preventive measures.

Major Findings

Majority (81%) are aware of online banking fraud. Legal awareness remains comparatively low (Mean = 3.12). Engineering students demonstrate higher awareness. Male students show slightly higher overall awareness. Internet usage positively influences awareness.

Suggestions

- There is a strong need to introduce mandatory cyber safety modules in undergraduate programs to enhance students' awareness of digital risks. Such modules will help students understand various cyber threats and safe online practices. This initiative will ensure that all undergraduates develop essential cyber hygiene and security knowledge. Conduct periodic cyber awareness workshops.
- It is important to establish campus cyber grievance cells in educational institutions to address cyber-related issues faced by students. These cells will provide a formal platform for reporting and resolving cybercrimes effectively. This initiative will help ensure timely support, awareness, and protection within the campus environment.
- There is a need to promote awareness of national cybercrime helplines and online reporting portals among students. This will help them understand where and how to report cyber incidents promptly. Such awareness will encourage timely action and improve response to cybercrime cases.
- Special awareness initiatives should be designed for non-technical students to improve their understanding of cyber safety concepts. These programs will simplify technical aspects and make cyber awareness more accessible. This will ensure equal knowledge distribution and better protection for all student groups.

4. Conclusion

The study reveals a moderate level of cybercrime awareness among undergraduate students in Tiruchirappalli District. Students show a reasonable understanding of common cyber threats such as phishing, hacking, and online fraud. However, their awareness of legal provisions

related to cybercrime is relatively low. Knowledge about reporting mechanisms and cybercrime helplines is also found to be insufficient. Technical awareness among students is comparatively better than their legal literacy. Engineering and technical students demonstrate slightly higher awareness levels than non-technical students. Male students show marginally higher awareness compared to female students. Increased internet usage is associated with improved awareness levels. Despite this, gaps still exist in critical areas of cyber safety knowledge. Institutional support for cyber education remains limited in some colleges. There is a clear need for structured cyber awareness programs. Curriculum integration of cyber safety topics is essential. Overall, targeted interventions are required to enhance cyber resilience among youth.

Article Information

Disclaimer (Artificial Intelligence): The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

Competing Interests: Authors have declared that no competing interests exist.

References

[1] T. Riley and S. Manville. Digital threats and student awareness. *Journal of Global Cybersecurity*, 4(1):12–29, 2015.

[2] P. Pokhrel and B. Chhetri. Cyber awareness among undergraduates. *International Journal of Information Security Education*, 7(1): 62–76, 2019.

[3] R. Sharma and P. Singh. Cyber law awareness in Indian colleges. *Indian Journal of Cyber Education*, 2(2):44–59, 2020.

[4] S. Kumar and P. Rajan. Digital literacy and cyber awareness in Tamil Nadu. *Journal of Educational Informatics*, 12(1):98–117, 2024.

[5] V. Bhardwaj and R. Sharma. Gender perspectives in cyber awareness. *Journal of Information Behaviour*, 9(3):213–230, 2020.

[6] M. Lwin and L. Wing. Cybercrime reporting behaviour. *Cyberpsychology Review*, 11(2):118–136, 2018.

[7] J. Thomas and L. Varghese. Reporting behaviour among students. *International Journal of Digital Society*, 8(1):77–94, 2022.