AWARENESS OF DIGITAL EVIDENCE AND CYBER-LAWS AMONG STUDENTS: ANANALYTICALSTUDY.

ABSTRACT

The increasing reliance on digital technologies has significantly transformed communication, education, and information exchange while simultaneously intensifying the risks associated with cybercrime and digital security. This study investigates students' awareness of digital evidence and cyber laws, with particular emphasis on their understanding of legal frameworks, digital evidence, cybercrime reporting mechanisms, and cybersecurity practices. A descriptive cross-sectional research design employing a quantitative approach was adopted. Primary data were collected from 120 respondents using a structured questionnaire administered through Google forms. The collected data were analysed using descriptive statistical techniques, including frequencies and percentages.

The findings reveal that although a majority of respondents demonstrated general awareness of digital evidence and cyber laws, substantial deficiencies persist in their understanding of the Information Technology Act, 2000, digital evidence preservation, and official cybercrime reporting procedures. The Internet and social media emerged as the predominant sources of information, whereas formal educational institutions played a comparatively limited role in fostering legal and cybersecurity awareness. Furthermore, respondents strongly supported the integration of cyber law education into academic curricula and emphasized the need for practical training, awareness campaigns, and capacity-building initiatives. The study concludes that strengthening cyber law education and digital citizenship, enhancing cyber resilience, and equipping students with the knowledge required to navigate evolving cyber threats and legal challenges in the contemporary digital environment.

Key words: Digital Evidence, Cyber Laws, Cybercrime Awareness, Digital Literacy, Information Technology Act 2000.

INTRODUCTION

In today's fast-paced digital world, the way we communicate, learn, and interact has been revolutionized by the rapid advancements in information and communication technology. Students, in particular, are active participants in this digital landscape, utilizing smartphones, laptops, social media platforms, and online resources as integral parts of their daily lives. It affects how we communicate, learn, do business and interact with each other. Students use devices and the internet a lot for school, social media, online shopping and sharing information. While technology has made things easier and more accessible it has also made us more vulnerable to cyber threats and crimes (UNESCO, 2023; ENISA, 2022; Wall, 2007).

Cybercrimes like hacking, phishing, identity theft and online fraud are becoming more common. As we use technology more and more it is important to understand cyber laws and how digital evidence is used to investigate and prosecute cybercrimes. Digital evidence is information from computers, phones, social media, emails and other electronic devices. It is a part of modern criminal investigations and court cases (Casey, 2011).

Cyber laws are rules that govern what we can and cannot do online. In India the Information Technology Act of 2000 is the law that deals with cyber activities and crimes. Students need to know about cyber laws and digital evidence so they can use the internet safely and responsibly. This knowledge helps prevent cybercrimes and makes students aware of their rights and responsibilities(Wall, 2007).**Despite, the existence of legal provisions, many students remain unaware of the laws governing their online behaviour and the potential consequences of violating cyber regulations.**

Every online action, from sending emails to browsing websites, leaves behind digital footprints known as **digital evidence**. This electronic trail can be crucial in investigating cybercrimes and establishing facts in legal proceedings. As students play a significant role in the digital ecosystem, understanding digital evidence is becoming increasingly important for them.

Background of the Study

The rapid advancement of information and communication technologies has fundamentally transformed the way individuals communicate, learn, conduct business, and access information. Students are among the most active users of digital technologies, relying extensively on smartphones, computers, social media, online learning platforms, and digital financial services for academic and personal activities. Although these technological developments have enhanced connectivity and educational opportunities, they have also increased exposure to cybersecurity threats, cybercrime privacy breaches, and legal challenges. Consequently, understanding digital evidence and cyber laws has become essential for promoting safe, responsible, and legally compliant use of digital technologies among students (UNESCO, 2023; ENISA,2022; Wall, 2007).

Digital evidence comprising electronically stored information such as emails, social media communications, digital documents, browsing history, and metadata, has become indispensable in the investigation and prosecution of cybercrimes. Simultaneously, cyber laws, particularly the information Technology Act, 2000 in India, provide the legal framework for regulating cyberspace, protecting digital rights, and addressing offences such as hacking, identity theft, cyber fraud, and unauthorized access. Despite the increasing significance of these legal and technological concepts, existing research indicates that many students possess only a limited understanding of cyber laws, digital evidence preservation, and cybercrime reporting procedures, thereby highlighting a critical gap in legal and cybersecurity awareness (Casey 2011; Interpol, 2023; National Crime Records Bureau (2023).

In response to the growing complexity of cyber threats and emerging technologies such as artificial intelligence, cloud computing, blockchain, and the internet of things (IoT), strengthening digital literacy and cyber law education has become increasingly important. Educational institutions play a pivotal role in developing responsible digital citizenship by equipping students with the knowledge and skills required to navigate digital environments safely and ethically.

Therefore, assessing students' awareness of digital evidence and cyber laws is essential for identifying existing knowledge gaps and informing educational strategies, awareness of digital evidence and cyber laws is essential for identifying existing knowledge gaps and informing educational strategies, awareness programmes, and policy interventions aimed at enhancing cybersecurity awareness, legal literacy, and responsible digital behaviour (Ribble, 2015; UNESCO, 2023; Alharbi et al., 2023).

OBJECTIVES OF THE STUDY

1. To assess the level of awareness among students regarding digital evidence and its significance in cybercrime investigations.
2. To examine students' knowledge and understanding of cyber laws governing online activities and cyber offences.
3. To identify the various sources through which students acquire information about digital evidence and cyber laws.
4. To evaluate students' awareness of cybercrime reporting procedures and available legal support mechanisms.
5. To analyse the relationship between selected demographic variables and students' awareness of digital evidence and cyber laws.
6. To suggest appropriate measures for enhancing awareness and legal literacy regarding digital evidence and cyber laws among students.

RESEARCH METHODOLOGY

Research Design

The present study adopted a descriptive cross-sectional research design to assess students' awareness of digital evidence and cyber laws. The design was selected because it helps in understanding the existing level of awareness and knowledge among students regarding the study topic. Data were collected from respondents at a single point in time.

Research Approach

A **quantitative research** approach was used for the study. This approach enabled the collection of numerical data from students and facilitated the analysis of their awareness regarding digital evidence and cyber laws.

Population of the Study

The population of the study consisted of Undergraduate and Postgraduate,Teachers,Ph.D scholars, students studying in educational institutions. Students were chosen because they regularly use digital technologies and online platforms for educational and personal purposes.

Sampling Technique

A convenience sampling technique was employed for selecting the respondents. Participants who were available and willing to participate in the study were included in the sample.

Sample Size

The study was conducted among students.

Inclusion Criteria

The study included:

- Undergraduate students.
- Postgraduate students.
- Students willing to participate in the study.
- Students with access to digital devices and internet facilities.

Exclusion Criteria

The study excluded:

- Individuals who were not students.
- Incomplete questionnaire responses.
- Duplicate responses.
- Respondents who did not provide consent.

Sources of Data

Primary Data

Primary data were collected directly from students through a self-structured questionnaire prepared using Google Forms.

Research Instrument

A **self-structured questionnaire** was used as the research instrument. The questionnaire was prepared based on the objectives of the study and relevant literature.

The questionnaire consisted mainly of **closed-ended questions,** including multiple-choice, dichotomous (Yes/No), and awareness-related questions. These questions were designed to collect uniform responses and facilitate quantitative analysis. In addition, **one open-ended question was included at the end of the questionnaire to** allow respondents to provide suggestions and express their views regarding awareness of digital evidence and cyber laws.

The questionnaire consisted of two sections:

Section A: Demographic Information

- Age
- Gender
- Educational Qualification
- Course of Study

Section B: Awareness of Digital Evidence and Cyber Laws

- Awareness of digital evidence
- Knowledge of cyber laws
- Awareness of cybercrime reporting procedures
- Sources of information regarding cyber laws and digital evidence
- Cybersecurity awareness and practices

Data Collection Procedure

Data was collected through **Google Forms**. The questionnaire link was shared with students through online platforms. Before participating, respondents were informed about the purpose of the study and their **consent** was obtained. The responses received were compiled and organized for analysis.

Ethical Considerations

Participation in the study was voluntary. Respondents were informed about the purpose of the research before completing the questionnaire. Confidentiality and anonymity were maintained throughout the study, and the collected information was used only for academic purposes.

Data Analysis

The data collected through Google Forms were transferred to Microsoft Excel for analysis. Frequencies, percentages, tables, and charts were used to summarize and interpret the findings according to the objectives of the study.

RESEARCH GAP

Several studies have examined cybercrime awareness and digital literacy among students. However, few studies have focused on students' awareness of digital evidence and their understanding of cyber laws (Alharbi et al., 2023; Alotaibi & Furnell, 2022). Most existing studies emphasize general cybersecurity knowledge **without examining whether students understand the significance of digital evidence and cybercrime reporting procedures.**

There is limited research exploring the relationship between **awareness of digital evidence and knowledge of cyber laws among students particularly in the Indian educational context**. This gap highlights the need for a study to assess students' awareness levels and identify areas requiring educational intervention.

RESULTS AND DISCUSSION

1. **To assess the level of awareness among students regarding digital evidence and its significance in cybercrime investigations.**

The first objective of the study sought to assess the level of awareness among students regarding digital evidence and its significance in cybercrime investigations. The findings indicate that the respondents possess a generally satisfactory level of awareness of the concept of digital evidence. A substantial majority of the participants (84.2%) reported that they were familiar with the term “digital evidence”, demonstrating that most students have at least a basic understanding of its existence within the digital and legal environment. Furthermore, 76.5% of the respondents were aware that digital evidence can be presented and accepted in court proceedings, suggesting a moderate level of understanding regarding its legal significance in criminal investigations and judicial processes. However, awareness of the practical dimensions of digital evidence remained comparatively limited. Although 37.5% of the respondents correctly identified that digital evidence may originate from multiple sources, including mobile phones, computers, and social media platforms, a considerable proportion associated digital evidence with only a single source. This finding indicates that many students are still unaware of the diverse forms and evidentiary value of electronically stored information.

The respondents also demonstrated moderate confidence in their knowledge of digital evidence, with 50% rating their knowledge of digital evidence, with 50% rating their knowledge as “Good” and 35.8% as “Excellent,” while only a small proportion rated their knowledge as “Fair” or “Poor”. Although these findings reflect a positive level of self-perceived awareness, they also reveal a gap between general familiarity and comprehensive understanding of digital evidence, particularly concerning its identification, preservation, and forensic application in cybercrime investigations. The findings are consistent with previous studies, which report that while students generally possess basic digital literacy, their knowledge of digital evidence and forensic procedures remains limited (Casey, 2011; Alharbi et al., 2023; ENISA, 2022). Overall, the results suggest that students exhibit a moderate-to-high

level of awareness regarding digital evidence; however, strengthening programmes is essential to enhance their understanding of the role of digital evidence in cybercrime prevention, investigation, and the administration of justice.

2. To examine students' knowledge and understanding of cyber laws governing online activities and cyber offences.

The second objective of the study was to examine students' knowledge and understanding of cyber offences. The findings indicate that respondents possess a moderate level of awareness regarding the legal framework regulating cyberspace; however, important gaps remain in their understanding of specific legal provisions. The study revealed that 60% of the respondents were aware of the Information Technology Act, 2000, while the remaining 40% had no knowledge of the Act. Although the majority demonstrated familiarity with India's principal cyber legislation, the sizeable proportion of students lacking awareness indicates that knowledge of statutory provisions remains inadequate among the significant section of the study population. Since the Information Technology Act, 2000 forms the legal foundation for addressing cyber offences, electronic records, digital signatures, and cybersecurity-related issues, limited awareness of this legislation may reduce students' ability to recognise legal rights, responsibilities, and the consequences of the unlawful online activities.

The findings further revealed that 61.7% of the respondents were aware that cybercrimes can result in legal punishment, whereas 38.3% were unaware of the legal consequences associated with cyber offences. In terms of self-assessment, the majority of respondents (60%) rated their knowledge of cyber laws as "Good" followed by 19.2% who rated it as "Excellent." However, 17.5% considered their knowledge to be "Fair," and 3.3% reported "Poor" knowledge suggesting that a considerable proportion of students still lack confidence in their understanding of cyber legislation. These findings demonstrate that while students possess a basic understanding of cyber laws, their knowledge remains largely conceptual rather than comprehensive. The results are consistent with previous research indicating that university students generally exhibit moderate awareness of cyber laws but possess limited knowledge of specific legal provisions, digital rights, and regulatory mechanisms governing cyberspace (Alotaibi & Furnell, 2022; Alharbi et al., 2023; Interpol, 2023). Overall, the findings underscore the need for systematic cyber law education, curriculum integration, and awareness programmes to strengthen students' legal literacy, encourage responsible online behaviour, and enhance compliance with cyber regulations in an increasingly digital society.

3. To identify the various sources through which students acquire information about digital evidence and cyber laws.

The third objective of the study was to identify the various sources through which students acquire information about digital evidence and cyber laws. The findings indicate that digital platform serve as the predominant source of information among the respondents. The internet emerged as the primary source, accounting for 40% of responses, followed by social media platforms, which contributed 31.7%. In contrast, educational institutions accounted for only

16.7% of the reported sources, while television, newspapers, and friends and family each contributed only 5.8%. These findings demonstrate that students rely predominantly on online and technology-driven platforms for acquiring knowledge related to digital evidence and cyber laws, reflecting the increasing influence of digital media in shaping awareness and information seeking behaviour among young adults.

Although the widespread use of the Internet and social media provides students with rapid access to information, dependence on these informal sources may expose them to inaccurate, incomplete, or unverified legal information. The comparatively limited contribution of educational institutions suggests that formal academic environments have not yet assumed a sufficiently active role in promoting cyber law education and digital forensic awareness. This finding highlights an important educational gap, considering that institutions of higher education are expected to provide structured, authentic, and evidence-based knowledge on legal and cybersecurityissues.Theresults are consistent with previous studies, which report that students primarily depend on digital platforms for cybersecurity information, while formal educational interventions remain comparatively limited (ENISA, 2022; UNESCO, 2023; Alharbi et al., 2023). Overall, the findings emphasize the need for educational institutions to strengthen curriculum-based cyber law education, integrate digital evidence concepts into academic programmes, and complement online information sources with structured awareness initiatives, workshops, and practical training to enhance students' legal literacy and responsible digital behaviour.

4. To evaluate students' awareness of cybercrime reporting procedures and available legal support mechanisms.

The fourth objective of the study was to examine students' awareness of cybercrime experiences, reporting mechanisms, and the need for educational interventions related to digital evidence and cyber laws. The findings reveal that although a majority of respondents (63.9%) had not personally experienced cybercrime, a considerable proportion (36.1%) reported being victims of cyber-related offences, indicating that cyber threats constitute a significant concern among students. Among the various forms of cybercrime, online fraud emerged as the most recognised offence (26.9%), followed by hacking (25.2%), phishing (22.7%), identity theft (16.0%), and cyberbullying (9.2%). These findings suggest that students are relatively more familiar with financially motivated and technologically driven cyber offences, likely due to their frequent exposure through digital media and personal online activities. However, despite this general awareness, practical knowledge regarding cybercrime reporting remained inadequate. A majority of respondents (61.3%) reported that they were unaware of the appropriate procedures for reporting cybercrime incidents, while appropriate procedures for reporting cybercrime incidents, while only 38.7% indicated familiarity with available reporting mechanisms such as the National Cyber Crime Reporting Portal, Cyber Crime Helpline1930, and Cyber Police Stations. This disparity highlights a critical gap between awareness of cyber threats and the practical ability to seek legal remedies and institutional support.

The findings further demonstrate a positive attitude among students towards strengthening cyber law education and awareness initiatives. Nearly two-thirds of the respondents (62.5%) had previously attended a cyber security or

cyber law awareness programme, reflecting moderate institutional outreach. More importantly, an overwhelming majority supported the inclusion of cyber law education within academic curricula (81.5%) and emphasized the need for additional awareness programmes on digital evidence and cyber laws (82.5%). Respondents further recommended workshops, seminars, practical training sessions, curriculum integration, social media campaigns, and regular awareness initiatives as effective strategies for improving knowledge and promoting responsible digital behaviour. These findings indicates that students recognize the importance of structured educational interventions in enhancing cybersecurity awareness, digital evidence literacy, and legal understanding. The results are consistent with previous studies, which emphasize that awareness programmes, curriculum integration, and experiential learning significantly improve students' cybersecurity knowledge and responsible online practices (Alharbi et al., 2023; ENISA, 2022; UNESCO, 2023). Overall, the findings underscore the need for collaborative efforts among educational institutions, policymakers, law enforcement agencies, and cybersecurity professionals to strengthen cyber law education, improve awareness of reporting mechanisms, and equip students with the practical competencies required to navigate an increasingly complex digital environment.

5. To analyse the relationship between selected demographic variables and students' awareness of digital evidence and cyber laws.

The fifth objective of the study was to identify appropriate measures for enhancing students' awareness of digital evidence and cyber laws. The findings demonstrate a strong consensus among respondents regarding the need for structured educational initiatives to improve cyber law literacy and digital awareness. A substantial majority of the respondents supported the inclusion of cyber law education within the academic curriculum (81.5%) and emphasized the necessity for additional awareness programmes related to digital evidence and cyber laws (82.5%). Furthermore, 62.5% of the respondents had previously attended cyber security or cyber security or cyber law awareness programmes, indicating that although awareness initiatives are being conducted, their coverage and effectiveness require further expansion to reach a wider student population. These findings reflect students' recognition that formal education plays a crucial role in developing responsible digital behaviour and strengthening legal awareness in an increasingly technology-driven society.

The respondents also proposed several practical strategies for improving awareness. Conducting workshops, seminars, and awareness programmes emerged as the most preferred measure (40%) followed by integrating cyber law and digital safety into the academic curriculum (24%), Other recommendations included the use of social media and online programs for awareness campaigns (16%), organizing practical training sessions and demonstrations (12%), and providing regular updates and informational campaigns on cyber laws (8%). These responses indicate that students favour a combination of theoretical instruction, experiential learning, and technology-enabled awareness initiatives to enhance their understanding of cyber laws and digital evidence. The findings are consistent with previous research, which suggests that curriculum integration, practical training, and continuous awareness programmes significantly improve cybersecurity knowledge, digital literacy, and responsible online behaviour among

students (ENISA, 2022; UNESCO, 2023; Alharbi et al., 2023). Overall, the findings underscore the importance of collaborative efforts involving educational institutions, government agencies, legal professionals, and cybersecurity experts to develop comprehensive awareness programmes that equip students with the knowledge and practical skills necessary to respond effectively to emerging cyber threats and legal challenges.

6. To suggest appropriate measures for enhancing awareness and legal literacy regarding digital evidence and cyber laws among students.

The sixth objective of the study sought to suggest appropriate measures for enhancing students' awareness and legal literacy regarding digital evidence and cyber laws. The findings indicate a strong consensus among respondents that existing awareness initiatives should be strengthened through systematic educational interventions. A substantial majority of the respondents supported the inclusion of cyber law education within the academic curriculum (81.5%) and expressed the need for additional awareness programmes focusing on digital evidence and cyber laws (82.5%). Although 62.5% of the respondents had previously participated in cyber security or cyber law awareness programmes, a considerable proportion had not received any formal exposure to such initiatives. This finding suggests that while awareness programmes have made a positive contribution, their reach and effectiveness remain insufficient to ensure comprehensive legal literacy among students. The results further indicate that students recognize formal education as an effective means of developing a sound understanding of cyber laws, responsible online behaviour, and the legal implications of digital activities.

The respondents also proposed several practical measures to strengthen awareness and legal literacy. Conducting workshops, seminars, and awareness programmes was identified as the most effective strategy (40%), followed by integrating cyber law and digital safety into academic curricula (24%). Additional recommendations included utilizing social media and online platforms for awareness campaigns (16%), organizing practical training sessions and demonstrations (12%), and conducting regular information campaigns on cyber laws and digital evidence (8%). These findings demonstrate that students favour a multi-disciplinary approach that combines classroom instruction, experiential learning, digital outreach, and continuous awareness activities. Such am approach would not only improve theoretical knowledge but also enhance practical competencies in cyber safety, digital evidence preservation, and cybercrime reporting. The findings are consistent with existing literature, which emphasizes that curriculum integration, experiential learning, stakeholder collaboration, and continuous awareness programmes significantly improve cybersecurity awareness, digital literacy, and legal compliance among students (ENISA, 2022; UNESCO, 2023; Alharbi et al., 2023). Overall, the study suggests that strengthening institutional support promoting collaboration between educational institutions and cybersecurity agencies, and implementing structured legal awareness programmes are essential for

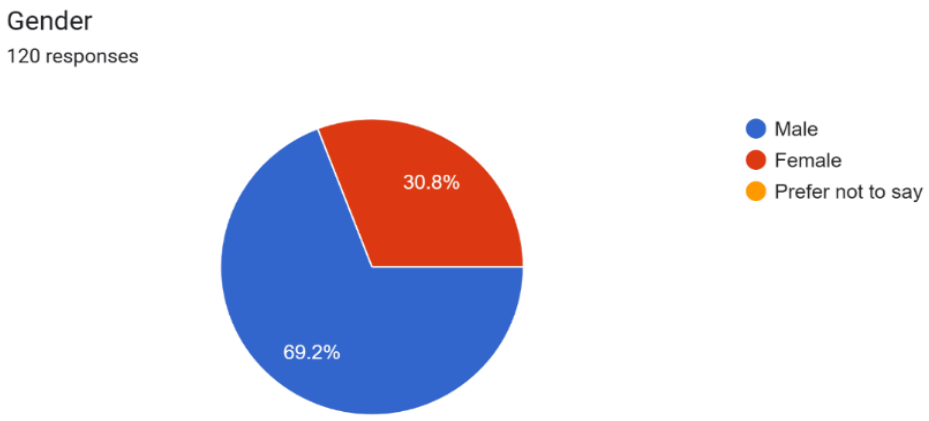
developing digitally responsible, legally informed, and cyber-resilient students capable of navigating the challenges of an increasingly digital society.

- **For the purpose of illustration, three completed questionnaires along with its corresponding analysis and interpretation is presented below. This example demonstrates the analytical procedure adopted in the study. The same process of coding, analysis and interpretation was uniformly applied to all the remaining 22 questionnaires**.

SECTION A:DEMOGRAPHIC PROFILE QUESTION

TABLE -1: GENDER

Gender	**Percentage (%)**	**Number of Respondents (n)**
Male	69.2%	83
Female	30.8%	37
Prefer not to say	0.0%	0
Total	**100.0%**	**120**



Interpretation of Data:

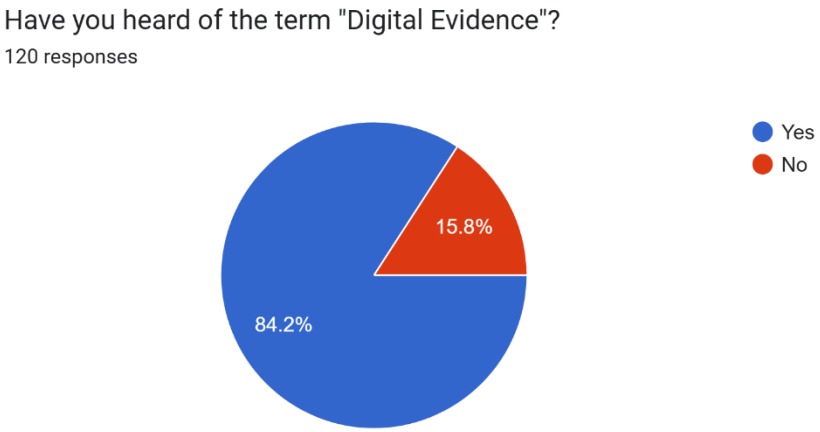
The findings suggest that the majority of participants were men, making up 69.2% (83 respondents) of the overall sample. Thirty-seven (30.8%) of the respondents were women. None of the participants chose the "Prefer not to say" option for their gender.This distribution suggests that the research sample was male-dominated, with males making up roughly two-thirds of the respondents.

SECTION B: AWARENESS OF DIGITAL EVIDENCE AND CYBER LAWS QUESTION

TABLE-8

Awareness of the Term "Digital Evidence" (n = 120)

Response	**Percentage (%)**	**Frequency (n)**
Yes	84.2%	101
No	15.8%	19
Total	**100.0%**	**120**



Interpretation of Data:

The provided data illustrates the level of awareness regarding the term "Digital Evidence" among a sample size of 120 respondents. The findings reveal a significant majority, with 84.2% (n=101) of participants indicating they are familiar

with the term. In contrast, only a small segment of the group, representing 15.8% (n=19), reported having no prior knowledge of it. These results signify a strong prevailing awareness of digital evidence within the surveyed population.

TABLE-25

Measures Suggested to Improve Awareness of Digital Evidence and Cyber Laws Among Students (50 Responses).

Sl. No.	Suggested Measures	Number of Responses	Percentage (%)
1	Conduct workshops, seminars, and awareness programmes	20	40.0
2	Include cyber laws and digital safety topics in the academic curriculum	12	24.0
3	Use social media and online platforms to spread awareness	8	16.0
4	Organize practical training sessions and demonstrations	6	12.0
5	Provide regular updates and informational campaigns on cyber laws	4	8.0

Interpretation of Data:

Students' proposed ways to raise awareness of cyber laws and digital evidence are shown in the table. The most common approach for raising awareness and understanding of cyber-related issues, according to 40% of participants, was to organize workshops, seminars, and awareness programs. Around 24% of those polled advocated including digital safety and cyber legislation in the academic curriculum so that students may learn these subjects formally. Furthermore, 16% emphasized the value of utilizing social media and online platforms to spread information broadly and efficiently. While 8% suggested regular awareness campaigns and updates on cyber laws, a lesser percentage of respondents (12%) proposed practical training sessions and demonstrations. In conclusion, the study suggests that students favour a mix of instructional, applied, and technologically driven strategies to increase awareness of cyber legislation and digital evidence.

CONCLUSION

The present study assessed students' awareness of digital evidence and cyber laws and examined their understanding of cybercrime, reporting mechanisms, sources of information, and educational requirements related to digital safety. The findings indicate that students possess a moderate to high level of general awareness regarding digital evidence and cyber laws. Most respondents were familiar with the concept of digital evidence, recognized its significance in legal proceedings, and demonstrated basic knowledge of cyber laws and the legal consequences of cybercrime. However, important gaps were identified in their understanding of the Information Technology Act, 2000, the diverse sources and preservation of digital evidence, and official cybercrime reporting procedures, suggesting that their knowledge remains largely conceptual rather than comprehensive.

The study further revealed that the internet and social media are primary sources of information on digital evidence and cyber laws, whereas educational institutions contribute comparatively less to students' legal awareness. Although respondents exhibited reasonable awareness of common cyber threats, practical knowledge related to digital evidence handling, cybercrime reporting, and legal compliance was found to be inadequate. The findings also demonstrated strong support for integrating cyber law education into academic curricula, expanding awareness programmes, and providing practical training through workshops, seminars, and expert-led sessions. Collectively, these findings emphasize that strengthening institutional initiatives, curriculum-based legal education, and collaborative awareness programmes is essential for enhancing digital literacy, promoting responsible digital citizenship, improving cyber resilience, and equipping students with the legal and practical competencies required to navigate an increasingly technology-driven society.

ACKNOWLEDGMENT

I Dr. R.N. Mangoliexpress my sincere gratitude to both the co-authors Ms. Dadibai Asma Nazirahmed (Research Scholar) and Vishal Melgiri (M.sc Student), Department of Criminology and Forensic Science, Rani Channamma University, Belagavi, for their valuable assistance, continuous encouragement, insightful suggestions, throughout the planning, execution, and completion of this research. They contributed substantially to the research design, data collection, data analysis, interpretation of findings, and manuscript preparation. Their collective dedication and teamwork played a vital role in the successful completion of the study titled *"Awareness of Digital Evidence and Cyber Laws among Students."*

I also extend my heartfelt appreciation to all the students who voluntarily participated in this research by providing their valuable responses. Their cooperation and willingness to participate made the successful completion of this primary research possible.

Special thanks are extended to the faculty members, the Department of Criminology and Forensic Science, and Rani Channamma University, Belagavi, for providing the necessary academic support and conducive research environment throughout the study.

Finally, the authors express their gratitude to everyone who directly or indirectly contributed to the successful completion of this research.

REFERENCES

- https://comdev.pubmedia.id/index.php/comdev/os retrieval date:-14-06-2026
- https://www.indianjournalofcomputerscience.com/index.php/tcsj/article/view/172777 retrieval date:-14-06-2026
- https://journals.sagepub.com/doi/10.1177/21582440241228920 retrieval date:-14-06-2026
- https://www.researchgate.net/publication/379872485_Cyber_security_awareness_survey_Students_in_University_of_Kalyani retrieval date:-16-06-2026
- https://www.researchgate.net/publication/394579982_Cybercrime_Awareness_Among_Undergraduate_Students_A_Descriptive_Study retrieval date:-16-06-2026
- https://journals.ncert.gov.in/IJET/article/view/1768retrieval date:-20-06-2026
- Alharbi, S., et al. (2023). Cybersecurity awareness among university students: A systematic review. Education and Information Technologies, 28(4), 4215–4238.
- Alotaibi, F., & Furnell, S. (2022). Cybersecurity awareness and behavior among students in higher education institutions. Information & Computer Security, 30(2), 247–263.
- Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
- ENISA. (2022). Cybersecurity Education Initiatives and Awareness Raising. European Union Agency for Cybersecurity.
- Interpol. (2023). Global Cybercrime Trend Report 2023.
- National Crime Records Bureau. (2023). Crime in India Report 2023.
- Ribble, M. (2015). Digital Citizenship in Schools (3rd ed.). International Society for Technology in Education.
- UNESCO. (2023). Global Education Monitoring Report 2023: Technology in Education.
- Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.