

REVIEWER'S REPORT

Manuscript No.: IJAR- 58380

Title: Awareness of Digital Evidence and Cyber-Laws Among Students: An Analytical Study.

Recommendation:

Accept after minor revision

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality			✓	
Clarity			✓	
Significance	✓			

Reviewer's ID: Abdul Haseeb Mir

Detailed Reviewer's Report

The manuscript titled "Awareness of Digital Evidence and Cyber-Laws Among Students: An Analytical Study" addresses a highly contemporary and critical junction between technology, digital forensics, and legal literacy. In an era characterized by ubiquitous digital connectivity and a corresponding surge in cyber-related offenses, investigating how the youth—who represent the most active demographic in cyberspace—perceive and understand digital evidence and cyber legislation is of paramount academic and social importance. The study employs a descriptive, cross-sectional quantitative design to assess these parameters among a sample of one hundred and twenty student respondents, focusing specifically on their familiarity with the Indian Information Technology Act of 2000, digital evidence preservation, and cybercrime reporting mechanisms.

The primary significance of this study lies in its attempt to distinguish between general cybersecurity hygiene and the specific legal-forensic dimensions of digital interactions. While existing literature frequently clusters these concepts under the broad umbrella of digital literacy, this manuscript correctly recognizes that understanding what constitutes admissible digital evidence and knowing how to legally report an incident are separate, critical competencies. The finding that a large majority of students are aware of the term "digital evidence" but lack operational knowledge regarding its diverse sources and official reporting channels like the National Cyber Crime Reporting Portal or the 1930 Helpline is highly illustrative. It highlights a crucial policy and educational gap, proving that informal sources like social media and the internet are failing to provide structured, actionable legal literacy, thereby shifting the responsibility onto formal educational institutions to integrate these concepts into their core curricula.

Detailed Recommendations for Improvement

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Despite the inherent value of the research topic, the manuscript in its current form exhibits several severe structural inconsistencies, logical contradictions, and methodological gaps that must be systematically addressed before it can be considered for publication.

The most critical structural flaw lies in the execution of the fifth and sixth research objectives. The fifth objective is explicitly stated as "To analyse the relationship between selected demographic variables and students' awareness of digital evidence and cyber laws". However, the text under the fifth results section (lines 270–298) completely fails to address this objective. Instead of presenting cross-tabulations, chi-square analyses, or any other inferential statistical tests relating variables such as gender, age, or educational qualification to awareness levels, the section discusses "appropriate measures for enhancing students' awareness". This entire discussion is almost a verbatim duplication of the text found under the sixth results section (lines 299–332), which is meant to focus on suggesting appropriate measures. The authors have effectively omitted the demographic relationship analysis entirely and repeated the recommendations section twice under different headings. To resolve this, the authors must either conduct the necessary statistical analyses to evaluate how demographic factors influence awareness or remove the fifth objective entirely and re-align the section numbering and analysis accordingly.

Additionally, there is a major logical contradiction regarding the study's sample size and methodology. In the methodology section and the demographic tables, the sample size is clearly stated to be one hundred and twenty respondents. However, on page eleven (lines 334–340), the text states that three completed questionnaires are presented for illustration, and that "the same process of coding, analysis and interpretation was uniformly applied to all the remaining 22 questionnaires". Mathematically, three plus twenty-two equals twenty-five questionnaires. This massive discrepancy raises serious concerns about the integrity of the data and suggests that portions of the manuscript may have been carelessly copy-pasted from a different, smaller study or a pre-existing template. The authors must explain this contradiction and ensure that the narrative precisely reflects the actual analytical processes applied to all one hundred and twenty respondents.

Furthermore, the inclusion of raw questionnaire text, individual interpretation steps, and statements regarding "three completed questionnaires" being presented for illustration is highly irregular for a peer-reviewed journal article. This formatting is more aligned with an academic thesis or a project report. For a journal article, this illustrative scaffolding must be removed, and the results should be presented collectively and synthetically. The descriptive data should be condensed into comprehensive, professionally formatted tables, and the narrative should focus on interpreting the overall trends rather than explaining the basic mechanics of how a single question was coded.

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Methodologically, the reliance on convenience sampling significantly limits the generalizability of the findings. A sample of one hundred and twenty students from what appears to be a single department or university (implied by the acknowledgments to Rani Channamma University) cannot be broadly generalized as representative of "students" as a whole. The authors must address this limitation in the discussion section and adjust the title or abstract to more accurately reflect the localized scope of the study. Under the "Sample Size" subsection on page four, the text is also incomplete, simply stating, "The study was conducted among students," without actually specifying the final sample size of one hundred and twenty. This sentence must be completed.

Finally, the manuscript requires thorough editorial proofreading to correct numerous typographical and formatting errors. For example, the title contains a spacing error in "ANANALYTICALSTUDY," and line twenty-four contains the fragmented word "digita". There are also repeated sentences, such as the exact duplication of the phrase "awareness of digital evidence and cyber laws is essential for identifying existing knowledge gaps and informing educational strategies" in lines sixty-seven through sixty-nine. The reference list is highly inconsistent; it contains raw URLs with retrieval dates alongside formal APA citations, and these should be standardized to a consistent academic citation style.

Conclusion and Publication Recommendation

In conclusion, this manuscript addresses an essential and under-researched dimension of digital literacy among students, making a strong case for the integration of cyber law and digital forensics into higher education curricula. However, because of the structural duplication between the fifth and sixth objectives, the mathematical contradiction regarding the questionnaire sample size, and the inclusion of thesis-style raw illustrative text, the manuscript cannot be accepted in its current state.

I recommend that the manuscript be given a **Revision** decision. If the authors can successfully perform the demographic statistical analyses required by their fifth objective, resolve the data count discrepancy on page eleven, remove the raw illustrative questionnaire text, and rigorously proofread the document for grammatical and formatting errors, this paper has the potential to make a meaningful, publishable contribution to the field of digital safety and cyber law education.