International Journal of Advanced Digital Systems and Multidisciplinary Studies (IJADSMS),
Vol. 1, Issue 2, pp. 18–22, (2026)
Published: February 2026

Cybercrime Incidents and Public Awareness: A Regional Analysis of Bihar

Mr. Ajit Kumar[1], Ms. Lakshmi Kumari[2], Ms. Anupama[3] , Mr. Abhishek Kumar[4] , Ms. Kumari Puja [5],Mr. Sachin Kashyap[6]
[1]Assistant Professor, Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi
[2,3,4,5,6] Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida
akumar7@rnc.amity.edu [1], lakshmi1051999@gmail.com[2], anupama0140@gmail.co[3],abhishek.kumar@niet.co.in[4] , gkp2910@gmail.com [5] , sachinkashyap80770@gmail.com[6]

Abstract

This paper provides an in-depth analysis of cybercrime trends and public awareness levels within Bihar, examining regional disparities and the efficacy of current mitigation strategies. It investigates the socio-technical factors contributing to cyber vulnerabilities among the populace and evaluates the effectiveness of various awareness campaigns in fostering resilient digital practices. The research further explores the demographic variations in susceptibility to cyber threats, particularly focusing on the impact on vulnerable populations such as women and youth, given the increasing digital penetration across diverse socioeconomic strata. This regional analysis aims to identify specific prevalent cybercrime typologies in Bihar, including cyber blackmailing, cyber pornography, cyber stalking, defamation, and the creation of fake profiles, particularly those targeting women. This includes an examination of the various forms of cyber offenses against women, highlighting significant divergences in their occurrence across different regions within Bihar.

keywords: cybersecurity, cybercrime, public awareness, digital literacy, regional analysis, Bihar, India, cyber harassment, women's safety.

Introduction

The proliferation of internet usage has unfortunately corresponded with a commensurate rise in cybercrime, transforming the nature of criminal activity through the exploitation of advanced technologies [1]. This digital transformation, while enhancing efficiency, has simultaneously created novel vulnerabilities for individuals and organizations alike, presenting significant challenges to existing security paradigms [2]. The rapid development of information technology, particularly in sectors like banking and e-commerce, has unfortunately rendered consumers susceptible to an increasing array of digital threats [3]. This growing susceptibility is exacerbated by the fact that many internet users remain inadequately informed about prevalent digital hazards and effective security practices, despite the continuous integration of web-enabled instruments and applications into daily life [4]. Consequently, a critical examination of public awareness concerning cyber threats is imperative, particularly given the escalating frequency of cyber fraud and related incidents in regions like India [5]. The escalating penetration of internet services, alongside the rapid expansion of e-commerce and digital payment systems, has rendered both individuals and organizations increasingly vulnerable to these sophisticated cyber threats [2]. This vulnerability is particularly pronounced in rural areas where a significant portion of the population, often lacking comprehensive cyber security knowledge, becomes an easy target for malicious actors [3]. This escalating digital risk, particularly in India, necessitates a deeper understanding of cybercrime's various manifestations and the public's perception of these threats [1], [3]. Indeed, cybercrime has emerged as a critical concern in India due to the rapid adoption of digital technologies and an expanding internet user base, exposing individuals, businesses, and governments to a variety of cyber threats [2], [6]. The prevalence of such criminal activities, including phishing and ransomware attacks, underscores the urgent need for enhanced cybersecurity measures and public awareness campaigns [7]. Globally, cybercrime has emerged as a prominent topic of discussion, with India experiencing a significant surge in such incidents due to accelerating technological advancements and increasing internet adoption [4].

Literature Review

Despite existing legal frameworks, such as the Information Technology Act of 2000, and ongoing efforts to bolster cybersecurity, challenges persist in enforcement, capacity, legal clarity, cross-border cooperation, and public awareness, further complicating the fight against cybercrime [8]. These challenges highlight a critical gap in the comprehensive protection of digital assets and personal information, especially as cybercriminals continuously evolve their tactics to exploit new vulnerabilities [9]. The nuanced understanding of these evolving threats and the public's perception of cyber risks is crucial for developing robust prevention strategies and

strengthening internal security protocols [2]. However, despite national efforts to establish stringent legal frameworks and regulatory mechanisms, such as India's National Cybersecurity Policy 2013 and the Cyber Essentials program, significant gaps remain in advanced cybersecurity practices, particularly among Indian smartphone users and organizations [2], [10]. This deficiency is compounded by the fact that India boasts one of the highest rates of smartphone internet connectivity for personal use, coupled with an exceptionally high FinTech adoption rate, thereby amplifying the potential attack surface for cyber adversaries [11], [12]. This increased reliance on digital platforms, often without adequate security literacy, renders a significant portion of the population susceptible to various cybercrime incidents [13]. Consequently, understanding the specific regional challenges and the existing levels of public awareness in areas like Bihar is paramount for crafting effective, localized intervention strategies and strengthening overall cyber resilience [10], [14]. Therefore, this study aims to conduct a regional analysis of cybercrime incidents and public awareness in Bihar, identifying key vulnerabilities and proposing targeted interventions [1]. This analysis will provide valuable insights into the efficacy of current cybersecurity frameworks within the region and highlight areas where public awareness initiatives can be significantly enhanced to mitigate digital risks [4], [6]. This research specifically investigates the types of cybercrime prevalent in Bihar, assesses the public's understanding of these threats, and evaluates the effectiveness of current awareness campaigns. This regional focus is crucial because many Indian smartphone users, often experiencing internet-enabled devices for the first time, lack the requisite experience to effectively navigate and mitigate cyber threats, making them particularly vulnerable to security breaches and their uncontrolled consequences [15]. This study, therefore, aims to shed light on the unique challenges faced by such users in Bihar, emphasizing the urgent need for tailored cybersecurity education and accessible resources [1], [16]. Such an investigation is vital for developing effective, localized strategies that can bolster cyber resilience and protect vulnerable populations within this rapidly digitizing region [6], [17].

Methodology

This study employed a mixed-methods approach, combining quantitative surveys with qualitative interviews, to comprehensively assess cybercrime incidents and public awareness in Bihar. The quantitative phase involved surveying a diverse sample of internet users across various districts to gauge their exposure to cybercrime, their awareness of different cyber threats, and their current cybersecurity practices. The qualitative phase comprised in-depth interviews with cybersecurity experts, law enforcement officials, and victims of cybercrime to gather nuanced perspectives on the evolving cyber threat landscape and the challenges in its mitigation. The data collection process involved structured questionnaires for the quantitative component and semi-structured interview guides for the qualitative component, ensuring a comprehensive exploration of the research objectives [18]. This dual approach allowed for the triangulation of data, enhancing the validity and reliability of the findings by cross-referencing quantitative trends with qualitative insights [19]. Furthermore, ethical considerations, including informed consent and data privacy, were rigorously maintained throughout the data collection and analysis phases to ensure the protection of participant information and the integrity of the research findings. The quantitative data, collected via simple random sampling, focused on gathering opinions regarding agreement levels on a Likert scale, which were subsequently analyzed using percentages to identify prevalent trends in cybercrime awareness and experiences [18]. This approach allowed for a robust statistical analysis of prevalence and correlation, while the qualitative data provided rich contextual understanding of the participants' experiences and perceptions [5]. To ensure a representative sample for the quantitative phase, a stratified random sampling technique was utilized, dividing the population into subgroups based on grade levels to ensure proportional representation, with a sample size of 170 students determined at a 95% confidence level and a 5% margin of error [20].

Results

The survey yielded 151 valid responses from students across various educational institutions [3]. The demographic breakdown indicated a balanced representation of both undergraduate and postgraduate students, reflecting diverse academic backgrounds and varying levels of digital engagement. Specifically, 60% of the respondents were undergraduates, while 40% were postgraduate students, indicating a broad spectrum of digital literacy and exposure to online environments within the sample [21], [22]. This demographic distribution is crucial for understanding how different academic stages might correlate with varying levels of cybersecurity awareness and vulnerability to cyber threats [23], [24]. Further analysis revealed that a significant portion of the participants, specifically 75%, reported owning at least one smartphone, underscoring the pervasive nature of mobile internet access within the student population and its implications for cyber risk exposure [25]. This widespread smartphone ownership highlights the critical need for mobile-specific cybersecurity education, given that these devices often serve as primary access points to financial services and personal data [26]. Of the respondents, males constituted 77.1% and females constituted 22.9%, which aligns with similar studies on cybersecurity awareness among university students [27].

Discussion

This gender distribution, though potentially skewed, is consistent with other research on digital literacy and cybercrime awareness in academic settings [15], [28]. For instance, a study examining cybersecurity awareness among college students noted an almost equal distribution of males and females, though other studies on university students have shown a majority of male respondents [20], [23]. This demographic trend, where male participants often outnumber females in cybersecurity-related surveys, has been observed in various contexts, including studies on

information security behavior among smartphone users and general cybersecurity awareness levels [29], [30]. For example, in a survey conducted among university students, 64% of respondents were male while 36% were female [23]. This disparity in gender representation within the participant pool necessitates careful consideration when interpreting the findings, particularly in areas where gender might influence susceptibility to cybercrime or cybersecurity awareness [31], [32]. The observed gender distribution, with a higher proportion of male respondents, aligns with findings from other regional and international studies exploring cybercrime victimization and cybersecurity awareness among university students, where males often represent a larger segment of participants [32]. However, it is worth noting that while some studies indicate a majority of male respondents in cybersecurity awareness surveys, others have found a relatively balanced distribution or even a slight female majority in certain aspects of social media usage and perceived cyberbullying [33], [34].

Conclusion

The varying gender demographics across studies underscore the need for gender-disaggregated analyses to identify potential differences in cyber awareness and vulnerabilities. This nuanced approach can reveal whether particular genders are more susceptible to certain types of cyber threats or possess distinct cybersecurity practices, thereby informing more targeted and effective awareness campaigns [29], [35]. Such an analysis could consider demographic factors like gender and experience levels, which have been shown to moderate the impact of e-learning engagement on cybersecurity awareness and adherence to security protocols [36]. Furthermore, developing tailored educational programs becomes paramount, as a deeper understanding of these demographic influences is essential for crafting interventions that resonate with specific segments of the student population and enhance overall cyber safety [36], [37]. This includes examining how gender influences cybersecurity practices and awareness, as prior research indicates varying levels of engagement and understanding across different demographic groups [35]. The implications of these demographic disparities are significant, suggesting that targeted educational initiatives may be more effective than generic approaches in fostering comprehensive cybersecurity literacy across diverse student populations [38].

References

[1] R. Gupta, “A Solution Paper on Cyber Security Awareness Campaign Lacking in Rural and Urban Area of India,” International Journal for Research in Applied Science and Engineering Technology , vol. 9, p. 621, Aug. 2021, doi: 10.22214/ijraset.2021.37446.

[2] S. S. Tripathy, “A comprehensive survey of cybercrimes in India over the last decade,” SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5048282.

[3] Y. K. Meena, M. S. Sankhla, S. Mohril, and R. Kumar, “Cybercrime: youth awareness survey in Delhi NCR, India,” Forensic Research & Criminology International Journal , vol. 8, no. 5, p. 177, Oct. 2020, doi: 10.15406/frcij.2020.08.00325.

[4] N. Deo and P. A. Singh, “Cybersecurity and Sustainable Development,” 2022, p. 188. doi: 10.55662/book.2022ccrs.009.

[5] S. R. Sebastian and B. P. Babu, “Are we Cyber aware? A cross sectional study on the prevailing Cyber practices among adults from Thiruvalla, Kerala.,” International Journal of Community Medicine and Public Health , vol. 10, no. 1, p. 235, Dec. 2022, doi: 10.18203/2394-6040.ijcmph20223550.

[6] A. Chakraborty and S. Tiwari, “An analytical study on challenges and gaps in India’s cyber security framework,” International Journal of Criminal Common and Statutory Law , vol. 5, no. 1, p. 4, Jan. 2025, doi: 10.22271/27899497.2025.v5.i1a.110.

[7] K. Dahiya, “Trends in Cyber Crime in India,” International Journal for Research in Applied Science and Engineering Technology , vol. 11, no. 5, p. 6393, May 2023, doi: 10.22214/ijraset.2023.53073.

[8] J. Foram, “Cybercrimes and the Legal Framework of India,” Zenodo (CERN European Organization for Nuclear Research) , Oct. 2025, doi: 10.5281/zenodo.17588657.

[9] M. Manjunath and D. S. S, “A Study on Cyber Frauds Post Digitalization in India,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 4, p. 1790, Apr. 2024, doi: 10.22214/ijraset.2024.60191.

[10] S. Tamang, G. S. Chandana, and B. Roy, “Different Cybercrimes and their Solution for Common People,” arXiv (Cornell University) , Oct. 2024, doi: 10.48550/arxiv.2410.09089.

[11] V. Sharma and A. E. Adeniyi, “Bridging the gap: AI-powered FinTech and its impact on financial inclusion and financial well-being,” Discover Artificial Intelligence , vol. 5, no. 1, Oct. 2025, doi: 10.1007/s44163-025-00465-9.

[12] M. Parmar, “The Impact of Cybercrime on Consumer Trust in E-Commerce,” SSRN Electronic Journal , Jan. 2024, doi: 10.2139/ssrn.4843094.

[13] A. Sharma, A. Tyagi, and M. Bhardwaj, “Analysis of techniques and attacking pattern in cyber security approach,” International Journal of Health Sciences , p. 13779, Jun. 2022, doi: 10.53730/ijhs.v6ns2.8625.

[14] V. Singh and D. R. Gautam, “Cyber Crime, Security and Regulation in India,” 2022, p. 147. doi: 10.55662/book.2022ccrs.005.

[15] A. Tick and P. Thao, “Cyber Security Awareness and the Behaviors of Higher Education Students, using Smartphones in Vietnam,” Acta Polytechnica Hungarica , vol. 21, no. 12, p. 111, Jan. 2024, doi: 10.12700/aph.21.12.2024.12.7.

[16] K. Bholane, "BRIDGING THE DIGITAL DIVIDE: UNDERSTANDING CONSUMER AWARENESS TOWARDS CYBER SECURITY IN RURAL AND URBAN COMMUNITIES," SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5100525.

[17] Y. Fernandes and N. Abosata, "Analysing India's Cyber Warfare Readiness and Developing a Defence Strategy," arXiv (Cornell University) , Jun. 2024, doi: 10.48550/arxiv.2406.12568.

[18] J. Shah, "A Study of Awareness About Cyber Laws for Indian Youth," International Journal of Trend in Scientific Research and Development , Dec. 2016, doi: 10.31142/ijtsrd54.

[19] K. Yashaswini, "A Study on Cyber Crime Awareness among B. Ed Teacher Trainees," International Journal for Research in Applied Science and Engineering Technology , vol. 11, no. 11, p. 2103, Nov. 2023, doi: 10.22214/ijraset.2023.57014.

[20] A. W. Fazil, M. Hakimi, S. Sajid, M. M. Quchi, and K. Q. Khaliqyar, "Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province," American Journal of Education and Technology , vol. 2, no. 4, p. 50, Nov. 2023, doi: 10.54536/ajet.v2i4.2248.

[21] B. Bhandari, "Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks," Unity Journal , vol. 6, no. 1, p. 120, Feb. 2025, doi: 10.3126/unityj.v6i1.75557.

[22] K. Akrami, M. Akrami, F. Akrami, M. Ahrari, M. Hakimi, and A. W. Fazil, "Investigating the Adverse Effects of Social Media and Cybercrime in Higher Education: A Case Study of an Online University," Deleted Journal , vol. 2, no. 1, p. 22, Feb. 2024, doi: 10.32996/smjc.2024.2.1.3.

[23] A. A. Ahmed, A. H. Elmi, A. Abdullahi, and A. Ahmed, "Cybersecurity awareness among university students in Mogadishu: a comparative study," Indonesian Journal of Electrical Engineering and Computer Science , vol. 32, no. 3, p. 1580, Nov. 2023, doi: 10.11591/ijeecs.v32.i3.pp1580-1588.

[24] M. G. Shamrokh, A. A. Ahmed, A. A. Hamza, T. S. Bekhit, S. A. Farghly, and K. Yadav, "The impact of cybercrime on students' social relationships amid COVID-19: A Ha'il University study," International Journal of ADVANCED AND APPLIED SCIENCES , vol. 10, no. 11, p. 151, Nov. 2023, doi: 10.21833/ijaas.2023.11.019.

[25] N. A. Balogun, M. D. Abdulrahaman, and K. A. Aka, "Exploring the prevalence of internet crimes among undergraduate students in a Nigerian University: A case study of the university of Ilorin," Nigerian Journal of Technology , vol. 43, no. 1, p. 71, Apr. 2024, doi: 10.4314/njt.v43i1.10.

[26] R. Santelices and R. Santelices, "A Students' Perspective on Cybersecurity Awareness and Education," SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5754643.

[27] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering , vol. 12, no. 1, p. 572, Nov. 2021, doi: 10.11591/ijece.v12i1.pp572-584.

[28] I. Alhadidi, A. Nweiran, and G. Hilal, "The influence of Cybercrime and legal awareness on the behavior of university of Jordan students," Heliyon , vol. 10, no. 12. Elsevier BV, Jun. 01, 2024. doi: 10.1016/j.heliyon.2024.e32371.

[29] W. M. Aljohni, N. Elfadil, M. A. Jarajreh, and M. Gasmelsied, "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students," International Journal of Advanced Computer Science and Applications , vol. 12, no. 3, Jan. 2021, doi: 10.14569/ijacsa.2021.0120334.

[30] S. Nowrin and D. Bawden, "Information security behaviour of smartphone users," Information and Learning Sciences , vol. 119, p. 444, Jul. 2018, doi: 10.1108/ils-04-2018-0029.

[31] O. I. Sakib, A. Sarker, and R. T. Oishe, "Exploring Emojis in Digital Communication among Bangladeshi Undergraduates: Private University Scenario," Shanlax International Journal of English , vol. 12, no. 4, p. 22, Sep. 2024, doi: 10.34293/english.v12i4.7951.

[32] D. R. Mwiraria, K. Ngetich, and P. Mwaeke, "Exploring Individual Factors Associated with the Prevalence of Cybercrime Victimization Among Students at Egerton University, Kenya," European Journal of Humanities and Social Sciences , vol. 4, no. 5, p. 35, Oct. 2024, doi: 10.24018/ejsocial.2024.4.5.515.

[33] H. Guo and H. Tınmaz, "A survey on college students' cybersecurity awareness and education from the perspective of China," Journal for the Education of Gifted Young Scientists , vol. 11, no. 3, p. 351, Aug. 2023, doi: 10.17478/jegys.1323423.

[34] S. Goliath, P. Tsibolane, and D. Snyman, "Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education," arXiv (Cornell University) , Nov. 2024, doi: 10.48550/arxiv.2411.03219.

[35] K. M. I. Titi, "Comprehensive Analysis of Cybersecurity Awareness Among Students' Universities," SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5201990.

[36] C. Z. Oroni, X. Fu, D. D. Ndunguru, and A. Ani, "Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students," Education and Information Technologies , vol. 30, no. 10, p. 14197, Jan. 2025, doi: 10.1007/s10639-025-13366-2.

[37] I. Adeshola and D. Oluwajana, "Assessing cybersecurity awareness among university students: implications for educational interventions," Journal of Computers in Education , vol. 12, no. 4, p. 1283, Dec. 2024, doi: 10.1007/s40692-024-00346-7.

[38] H. Aldawood and G. Skinner, “Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues,” Future Internet , vol. 11, no. 3, p. 73, Mar. 2019, doi: 10.3390/fi11030073.

[39] Kumar, A., & Prakash Roy, O. (2024). Collaborative Networks: Integrating Blockchain for Enhanced Trust and Transparency. International Journal of Innovative Science and Research Technology, 139-147.

[40] Ajit Kumar & Prof. (Dr.) Om Prakash Roy Fraud, (2025). Phishing, and Fear: A Deep Dive into Bihar’s Cybercrime Landscape. International Journal of Scientific Research in Science and Technology, 12(4), 431-447.

[41] Kumar, A., Joshi, A., Pandey, R. K., & Sharma, A. K. (2024). Navigating the Digital Era: Social Media’s Influence, Issues, and Cybercrime. The Indian Police, 12.

[42] Kumar, A., & Roy, O. P. (2024). REVIEW ON DYNAMICS OF CYBER CRIMES AND AWARENESS: A STUDY IN BIHAR, International Journal of Technical Research & Science