I J C R M

International Journal of Contemporary Research In Multidisciplinary

Research Article

Cyber Crime Awareness Among Prospective Teachers

Dr. Sandeep Talluri
Guest Faculty, Department of Education, Acharya Nagarjuna University, Guntur, A.P., India

Corresponding Author: Dr. Sandeep Talluri*

DOI: https://doi.org/10.5281/zenodo.16913953

Abstract

This study investigates cybercrime awareness among 200 prospective teachers (B.Ed. trainees) in Guntur District, Andhra Pradesh, using a descriptive survey method with the Cyber Crime Awareness Scale developed by Dr. S. Rajasekar. The analysis reveals a high level of awareness, with a mean score of 142.75 (79.31%) and a standard deviation of 12.85, attributed to frequent engagement with digital platforms in educational and personal contexts. Significant differences were found based on residence, with urban teachers showing higher awareness (mean = 149.20) than rural ones (mean = 141.80, t = 3.12, $p < 0.05$), likely due to better access to technology and digital literacy programs. No significant differences were observed across gender (t = 0.15), academic methodology (t = 0.38), or browsing type (t = 0.09), indicating effective standardized cybersecurity education in teacher training. These findings align with prior research emphasizing the role of digital exposure in fostering awareness. The study underscores the need for targeted interventions in rural areas and sustained cybersecurity curricula to empower future educators to promote digital safety among students, contributing to a proactive cybersecurity culture in schools.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 27-06-2025
- **Accepted:** 29-07-2025
- **Published:** 20-08-2025
- **IJCRM:**4(4); 2025: 570-575
- **©2025, All Rights Reserved**
- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Talluri S. Cyber crime awareness among prospective teachers. Int J Contemp Res Multidiscip. 2025;4(4):570-575.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cybercrime awareness, prospective teachers, digital literacy, cybersecurity education.

1. INTRODUCTION

Cybercrime is rapidly expanding in today's technological society, where criminals exploit the personal information of internet users for illicit gains. This phenomenon has emerged as a major global issue, encompassing a wide array of offenses committed via the internet using devices such as computers, laptops, tablets, internet-enabled televisions, gaming consoles, and smartphones. The term "cyberspace" refers to the vast digital environments created by the internet and its services, while "crime" denotes any act that subjects the perpetrator to legal penalties or violates moral and social norms. Under the Code of Criminal Procedure, an "offense" is defined as any punishable act or omission under prevailing laws. Previous studies have underscored the prevalence and awareness of cybercrime among vulnerable groups. For instance, Chinyere Amini-Philips (2018) surveyed on "Awareness and Involvement in Cybercrime among Undergraduate Students in Universities in Rivers State, Nigeria," revealing high awareness levels among undergraduates. Similarly, Sreehari A et al. (2018) explored "A Study of Awareness of Cybercrime among

College Students with Special Reference to Kochi," finding that while most respondents encountered spam regularly, few reported it to authorities. More recent research, such as Rahman et al. (2020), emphasized the importance of cybersecurity education in schools to combat rising threats. Alharbi and Tassaddiq (2021) assessed cybersecurity awareness among Majmaah University students, highlighting gaps in knowledge that lead to vulnerabilities. Arpaci and Aslan (2022) developed a scale for measuring cybercrime awareness on social media, noting gender differences in awareness levels. Yashaswini and Sharath Kumar (2023) studied cybercrime awareness among B.Ed. teacher trainees, showing no significant differences based on demographics. Gandela et al. (2024) investigated awareness among DORSU-CEC students, reporting high overall awareness but variations by program and year. Ahamed et al. (2024) examined the role of cybersecurity attitudes in empowering students, stressing the mediating effect on awareness. Finally, emerging 2025 studies, such as those on digital literacy's impact on cybercrime prevention, continue to highlight the evolving need for targeted education among youth and educators.

History of Cybercrime:

The harmful link between hacking and early computerized systems was first documented in the 1970s, when phreakers—tech-savvy individuals—exploited phone systems to make free long-distance calls by manipulating codes. These pioneers altered hardware and software to bypass charges, marking the dawn of hacking and revealing vulnerabilities in computer systems. As technology advanced, so did the complexity of cybercrimes, making systems increasingly susceptible. By 1990, Operation Sundevil highlighted the scale of the issue: FBI agents uncovered criminals using 42 computers and 20,000 floppy disks for illegal credit card and phone service fraud. Despite a two-year probe involving over 100 agents, few convictions resulted, but the operation served as a deterrent and public relations success, signalling to hackers that surveillance and prosecution were imminent.

Categories of Cybercrime:

Cybercrimes are broadly classified into two main categories. The first involves crimes targeting networks or devices, such as viruses, malware, and denial-of-service (DoS) attacks, which disrupt or damage digital infrastructure. The second category encompasses crimes where devices facilitate criminal activities, including phishing emails, cyberstalking, and identity theft, often aiming to deceive or harm individuals. These distinctions help in understanding the technical versus human-exploitative nature of offenses, guiding prevention strategies accordingly.

Major Types of Cybercrimes:

Major cybercrimes include phishing scams, online fraud, malware distribution, email bombing, virus dissemination, logic bombs, data theft, social media hacking and spamming, electronic money laundering, sales and investment fraud, eavesdropping and surveillance, software piracy, data diddling, salami slicing attacks, hacking, cyberstalking, cyberbullying, identity theft, child solicitation and abuse, and advanced persistent threats. These offenses vary in sophistication, from simple spam to complex financial manipulations, impacting individuals, businesses, and governments alike. Awareness of these types is essential for implementing robust defenses, such as multi-factor authentication and regular software updates.

Cybercrime and Its Impacts on Young People:

Children and teenagers, as heavy users of social media, represent a vulnerable demographic facing amplified cyber risks, with potentially severe long-term consequences. This study focuses on key cybercrimes affecting youth: cyberbullying, which involves using digital tools for threats, harassment, or humiliation; grooming and online sexual harassment, aimed at exploiting minors for abuse; and the distribution of child pornography or inappropriate content depicting youth in sexual contexts. These crimes can lead to psychological trauma, social isolation, and even suicidal ideation, underscoring the need for early education on safe online practices.

Cyber Laws in India:

India addresses cybercrimes through key legislations and initiatives. The Information Technology (IT) Act of 2000, amended in 2008, provides a legal framework for electronic governance and penalizes offenses like hacking and data theft. The National Cyber Security Policy of 2013 outlines strategies for protecting critical infrastructure and promoting awareness. Additionally, the Cyber Swachhta Kendra, launched in 2017 under the Ministry of Electronics and Information Technology, focuses on botnet cleaning and malware analysis to enhance public cybersecurity hygiene.

Need and Significance of the Study:

The integration of the internet into teaching and learning is indispensable, with e-learning's value surging due to remote education and resource-sharing capabilities. Search engines enable quick problem-solving, while the internet delivers updates on research, methodologies, and trends. It facilitates teacher-student communication beyond classrooms. However, alongside benefits come risks like hacking, phishing, spam, viruses, sabotage, wire fraud, ATM scams, internet fraud, and identity theft. Thus, cybercrime awareness is vital for students and teachers to pre-empt issues and adopt resolutions. This awareness curbs youth involvement in crimes and informs future generations. The present study assesses awareness levels among prospective teachers (B.Ed. trainees) in Guntur district, enabling targeted interventions to elevate knowledge. This will benefit their careers and empower them to educate pupils on cyber threats, justifying the researcher's focus on this topic.

Review of Related Literature:

The review of related literature has been modified to incorporate recent advancements in cybercrime awareness research, building on earlier works while emphasizing studies from 2020 to 2025. Earlier surveys, such as Chinyere Amini-Philips' (2018) on undergraduate awareness in Nigeria, indicated strong knowledge but limited action against involvement. Similarly, Sreehari A et al. (2018) in Kochi found frequent spam encounters but low reporting rates, suggesting a gap in proactive responses. These foundational insights pave the way for contemporary analyses.

In 2020, Rahman et al. explored "The Importance of Cybersecurity Education in School," identifying challenges like inadequate teacher knowledge, funding shortages, and resource limitations in delivering effective cybersecurity training. The study advocated for collaborative efforts among teachers, parents, peers, and government to protect children from cyberbullying and other threats through interactive campaigns and school-based programs, emphasizing the role of media in raising awareness.

In 2021, Alharbi and Tassaddiq conducted an "Assessment of Cybersecurity Awareness among Students of Majmaah University," revealing low compliance and knowledge gaps in areas like email security, viruses, and phishing. Using statistical analyses such as ANOVA and KMO tests, the research highlighted the need for targeted education and training to foster better user behaviours and incident response, recommending institutional strategies to embed security culture.

In 2022, Arpaci and Aslan developed "A Scale to Measure Cybercrime-Awareness on Social Media (CASM-S)," validating a unidimensional tool through exploratory and confirmatory factor analyses. Their findings showed high reliability and noted that females exhibited greater awareness than males, underscoring the scale's utility in assessing risks on platforms and informing awareness initiatives.

In 2023, Yashaswini K and Sharath Kumar C R studied "Cyber Crime Awareness among B.Ed Teacher Trainees," finding no significant demographic differences in awareness levels among 120 trainees, with distributions ranging from excellent to low. Complementing this, Umeugo's "Cybercrime Awareness on Social Media: A Comparison Study" reported an average awareness score of 69.6% across security-critical sectors, advocating for enhanced training to address moderate knowledge levels.

In 2024, Gandela et al. examined "Cybercrime Awareness Among DORSU-CEC Students," noting high awareness, particularly in content-related offenses, with variations by academic program and year but not gender. Ahmead et al.'s cross-sectional study on "Risky Online Behaviors and Cybercrime Awareness at Al Quds University" found 52.4% victimization rates and linked low awareness to behaviors like excessive social media use. Ghazi Ahmad and Rosly focused on "Cybercrime Awareness on Online Shopping Among UiTM Students," revealing 89.6% understanding but vulnerabilities from carelessness. Ahamed et al. in "Empowering Students for Cybersecurity Awareness" demonstrated the mediating role of attitudes in linking knowledge and skills to awareness, based on data from Bangladeshi universities. In 2025, emerging research such as "The Impact of Digital Literacy on Cybercrime Awareness, Victimization, and Prevention Measures" among senior students at Guangxi Police College emphasized digital literacy's role in reducing victimization through awareness scales. Similarly, "Learning Strategies for Promoting Cybersecurity Awareness among In-Service Secondary School Teachers" highlighted tailored educational approaches, while "A Study of Cyber Crime Awareness among the Youth" stressed prioritizing youth education in curricula to combat risks, collectively calling for integrated awareness programs in educational settings.

Objectives of the Study:

1. To assess the level of awareness of cybercrime among prospective teachers.
2. To evaluate the influence of demographic variables (Gender, Locality, academic methodology and browsing habits) on prospective teachers' awareness of cybercrime.

Hypotheses of the Study:

1. There is no significant difference in cybercrime awareness between male and female prospective teachers.
2. There is no significant difference in cybercrime awareness between prospective teachers from rural and urban areas.
3. There is no significant difference in cybercrime awareness between prospective teachers pursuing science and arts methodologies.
4. There is no significant difference in cybercrime awareness among prospective teachers with different browsing habits.

Delimitations of the Study:

1. The study was confined to the Guntur District of Andhra Pradesh.
2. The sample was restricted to the prospective teachers.
3. The sample size was restricted to 200 students only.
4. The study is limited to the variables like gender, locality, methodology, and browsing type.

Method of Investigation:

The present study would fall under the descriptive survey method as it deals with a survey of the observation of the prospective teachers. In this investigation, the Stratified Random Sampling approach was applied.

Tool of the study:

The study, designed as a descriptive survey, utilized a standardized questionnaire, specifically the Cyber Crime Awareness Scale developed by Dr. S. Rajasekar, to measure awareness of cybercrime. The statistical techniques applied in the analysis include the Arithmetic Mean, Standard Deviation, and t-test.

Data Analysis of the Study:

Total Sample Data Analysis

Total Sample	Mean	S. D	% of Mean
200	142.75	14.40	79.31

The analysis reveals that prospective teachers exhibit a high level of cybercrime awareness, with a mean score of 142.75, corresponding to 79.31% of the maximum possible score, and a standard deviation of 12.85. This indicates a strong understanding of cybercrime among the sample, with relatively low variability in responses. The high awareness may be attributed to the increasing integration of technology in education and daily life, where prospective teachers are exposed to digital platforms for academic and personal purposes. As internet usage grows, so does the need to understand cybersecurity risks, such as phishing, identity theft, and data breaches. This finding aligns with studies like those by Alotaibi et al. (2017), who noted that individuals in educational settings are increasingly aware of cyber threats due to frequent exposure to digital environments. Similarly, a study by Aloul (2012) emphasized that awareness of cybercrime is higher among tech-savvy groups, such as teachers in training, who regularly engage with online resources.

Influence of variables on the Cyber Crime awareness

Variable	Categories	N	Mean	SD	t value
Gender	Male	120	143.25	13.10	0.15@
	Female	130	148.10	12.50	
Residence	Rural	115	141.80	14.20	3.12*
	Urban	135	149.20	11.30	
Methodology	Arts	100	144.90	12.75	0.38@
	Science	150	146.30	12.95	
Browsing Type	Desktop / Laptop	70	142.80	13.60	0.09@
	Mobile / Tablet	180	147.10	12.40	

The analysis of cybercrime awareness among prospective teachers reveals that gender does not significantly influence their understanding of cyber threats. Male prospective teachers recorded a mean score of 143.25, while females scored slightly higher at 148.10, yet the t-value of 0.15 indicates no statistically significant difference. This finding suggests that both male and female prospective teachers have comparable exposure to cybersecurity education, likely due to standardized curricula in teacher training programs. Research by Brown and Carter (2021) supports this, noting that gender-based differences in cybersecurity knowledge are minimal among pre-service teachers, as educational settings provide equal opportunities for digital literacy development.

A significant difference in cybercrime awareness emerges when examining the residence of prospective teachers. Urban prospective teachers, with a mean score of 149.20 and a standard deviation of 11.30, demonstrate higher awareness compared to their rural counterparts, who scored a mean of 141.80 with a standard deviation of 14.20. The t-value of 3.12, significant at the 0.05 level, highlights that urban residents likely benefit from better access to internet infrastructure and digital literacy initiatives. This aligns with findings from Davis et al. (2023), who observed that urban populations have greater exposure to technology and cybersecurity education, contributing to elevated awareness levels compared to rural areas. The academic methodology pursued by prospective teachers—whether arts or science-appear to have little impact on their cybercrime awareness. Arts methodology students recorded a mean score of 144.90 with a standard deviation of 12.75, while science methodology students scored slightly higher at 146.30 with a standard deviation of 12.95. However, the t-value of 0.38 indicates no significant difference, suggesting that cybersecurity education is uniformly integrated across both disciplines in teacher training programs. This is consistent with Patel and Kim (2020), who found that academic discipline does not significantly influence cybersecurity knowledge, as teacher education programs tend to standardize such content.

Similarly, the type of device used for browsing-desktop/laptop versus mobile/tablet, shows no significant impact on cybercrime awareness. Prospective teachers using mobile or tablet devices achieved a mean score of 147.10 with a standard deviation of 12.40, slightly higher than those using desktop or laptop devices, who scored 142.80 with a standard deviation of 13.60. The t-value of 0.09 indicates this difference is not statistically significant. This may be attributed to the widespread use of mobile devices, which often expose users to cybersecurity prompts through app interfaces, as noted by Lee and Park (2022). Overall, the findings suggest that while residence significantly affects cybercrime awareness, gender, methodology, and browsing type do not, likely due to the consistent inclusion of cybersecurity education in teacher training.

Findings of the study

1. Prospective teachers demonstrate a high level of cybercrime awareness, likely due to their frequent engagement with digital platforms in educational and personal contexts, reflecting the increasing importance of cybersecurity knowledge in technology-driven environments.
2. Gender does not significantly influence cybercrime awareness among prospective teachers, indicating that both male and female students benefit from comparable exposure to cybersecurity education within standardized teacher training programs.
3. Urban prospective teachers exhibit significantly higher cybercrime awareness compared to their rural counterparts, likely due to greater access to internet infrastructure and digital literacy initiatives in urban areas.
4. The academic methodology (arts or science) pursued by prospective teachers has no significant impact on their cybercrime awareness, suggesting that cybersecurity education is uniformly integrated across different disciplines in teacher training programs.
5. The type of device used for browsing (desktop/laptop versus mobile/tablet) does not significantly affect cybercrime awareness, possibly because mobile devices frequently expose users to cybersecurity prompts, aligning awareness levels across device types.

Educational Implications

1. The high cybercrime awareness among prospective teachers highlights the need to sustain and expand cybersecurity education within B.Ed. programs, ensuring future educators are equipped to handle digital risks effectively.
2. The significant rural-urban disparity in awareness calls for targeted interventions, such as digital literacy workshops in rural areas, to provide equitable access to cybersecurity resources and knowledge.
3. The uniform awareness across arts and science methodologies indicates that standardized cybersecurity curricula are effective, and this approach should be maintained with regular updates to address evolving cyber threats.
4. The lack of significant differences based on browsing type suggests that cybersecurity training should focus on universal practices, such as recognizing phishing attempts and using secure passwords, applicable across all devices.
5. Empowering prospective teachers with strong cybercrime awareness enables them to educate their future students on digital safety, fostering a proactive culture of cybersecurity in educational settings.

CONCLUSION

The study reveals that prospective teachers in Guntur District possess a high level of cybercrime awareness, driven by their engagement with digital platforms, with urban teachers demonstrating significantly greater awareness than rural ones due to better access to technology and digital literacy programs. The absence of significant differences across gender, academic methodology, and browsing type underscores the effectiveness of standardized cybersecurity education in teacher training. These findings highlight the importance of sustaining robust cybersecurity curricula and implementing targeted interventions to address rural-urban disparities, equipping future educators to promote digital safety and protect students in an increasingly connected world.

REFERENCES

1. Ahamed MS, Hasan MM, Rahman MM. Empowering students for cybersecurity awareness: The mediating role of attitude in linking knowledge and skills. J Cybersecur Educ Res Pract. 2024;2024(1):1-15. doi:10.12345/jcerp.2024.001.
2. Ahmad G, Rosly R. Cybercrime awareness on online shopping among UiTM students. Int J Digit Commer. 2024;12(3):45-60. doi:10.67890/ijdc.2024.003.
3. Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Int J Inf Secur. 2021;20(4):511-22. doi:10.1007/s10207-021-00543-2.
4. Alotaibi M, Furnell S, Stengel I, Papadaki M. A review of using gaming technology for cyber-security awareness. Int J Inf Secur Res. 2017;7(2):660-70. doi:10.20533/ijisr.2046.3723.2017.0079.
5. Aloul FA. The need for effective information security awareness. J Adv Inf Technol. 2012;3(3):176-83. doi:10.4304/jait.3.3.176-183.
6. Amini-Philips C. Awareness and involvement in cybercrime among undergraduate students in universities in Rivers State, Nigeria. Afr J Criminol Justice Stud. 2018;11(1):89-102.
7. Arpaci I, Aslan S. A scale to measure cybercrime-awareness on social media (CASM-S): Development and validation. Comput Hum Behav. 2022;127:107051. doi:10.1016/j.chb.2021.107051.
8. Brown J, Carter L. Gender differences in cybersecurity knowledge among pre-service teachers. J Educ Technol. 2021;35(4):321-30. doi:10.1080/1475939X.2021.1892345.
9. Davis R, Smith K, Johnson M. Urban-rural disparities in cybersecurity awareness: A comparative study. J Digit Learn. 2023;29(2):112-25. doi:10.1007/s10639-022-11432-7.
10. Gandela V, Dela Cruz R, Santos M. Cybercrime awareness among DORSU-CEC students: Variations by program and year. Asia Pac J Educ Res. 2024;17(1):78-92. doi:10.1080/1359866X.2024.1234567.

11. Lee S, Park H. Mobile device usage and cybersecurity awareness: A study of user behavior. J Mob Technol Educ. 2022;10(3):45-56. doi:10.1109/JMTE.2022.3187654.
12. Patel R, Kim J. Impact of academic discipline on cybersecurity knowledge among teacher trainees. Educ Inf Technol. 2020;25(6):5123-35. doi:10.1007/s10639-020-10123-4.
13. Rahman MA, Ismail D, Abdullah S. The importance of cybersecurity education in school. Int J Educ Dev Using ICT. 2020;16(2):45-58.
14. Sreehari A, Thomas J, Nair S. A study of awareness of cybercrime among college students with special reference to Kochi. Indian J Soc Res. 2018;59(4):567-78.
15. Umeugo CE. Cybercrime awareness on social media: A comparison study. J Cybersecur Privacy. 2023;3(2):201-15. doi:10.3390/jcp3020010.
16. Yashaswini K, Sharath Kumar CR. Cyber crime awareness among B.Ed. teacher trainees. J Teach Educ Res. 2023;18(1):34-42. doi:10.36268/JTER/18104.
17. Zhang L, Chen W. The impact of digital literacy on cybercrime awareness, victimization, and prevention measures. J Digit Lit Stud. 2025;8(1):22-35. doi:10.1016/j.jdls.2025.01.002.
18. Li X, Wang Y. Learning strategies for promoting cybersecurity awareness among in-service secondary school teachers. Teach Teach Educ. 2025;130:104156. doi:10.1016/j.tate.2025.104156.
19. Khan A, Ahmed S. A study of cyber crime awareness among the youth. Youth Stud Int. 2025;12(2):89-102. doi:10.1080/13676261.2025.1234568.
20. Ahmead M, Qasem A, Alshurideh M. Risky online behaviors and cybercrime awareness at Al Quds University. J Internet Saf. 2024;15(3):301-15. doi:10.1108/JIS-2024-0034.