International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 10 Issue 1, Jan-Feb, 2022, Impact Factor: 7.326

Cybercrime Awareness Among College Students: A Comparative Study of Gender and Locality

Dr. Sunil Kumar

Associate Professor, Department of Psychology, Pt. NRS Government College, Rohtak

ABSTRACT

The expansion of internet-based education, communication, banking, social networking, and digital services has increased both the opportunities and the risks associated with online participation. College students constitute a particularly important group because they are intensive users of digital technologies and may encounter phishing, identity theft, cyberstalking, hacking, malware, online fraud, privacy violations, and other cyber-enabled harms. The present study examined cybercrime awareness among 100 college students from Rohtak district, comprising 50 males and 50 females, with additional comparison by locality (urban and rural). A descriptive survey design was employed and cybercrime awareness was assessed using the Cyber Crime Awareness Scale (CCAS-RS) developed by S. Rajasekar (2013). Mean, standard deviation, and independent-samples t tests were used for analysis. Male students (M = 141.42, SD = 25.15) obtained a slightly higher mean awareness score than female students (M = 134.75, SD = 41.92), but the difference was not statistically significant, t(98) = 1.81, p ≈ .073, Cohen's d ≈ 0.19. Urban students (M = 152.82, SD = 24.75) scored significantly higher than rural students (M = 140.51, SD = 19.76), t(98) = 2.09, p ≈ .039, Cohen's d ≈ 0.55. The findings are interpreted in relation to research published between 2000 and 2021, including work on information-security awareness, student vulnerability, gender, and the digital divide. The study suggests that cybercrime awareness among college students is better understood as a function of exposure, digital access, educational opportunities, and security knowledge than of gender alone. Structured cyber-safety education, especially for students from less digitally resourced settings, is recommended.

Keywords: cybercrime awareness, cybersecurity, college students, gender, locality, digital literacy, rural-urban divide, cyber safety, CCAS-RS

INTRODUCTION

Digital technologies have transformed higher education and everyday life. Internet-enabled communication, social networking, digital payments, cloud services, online learning, and mobile applications have expanded access to information and services, but they have also created new opportunities for deception, unauthorized access, identity misuse, privacy invasion, and technology-facilitated harassment. Cybercrime therefore represents not only a technical problem but also an educational, behavioural, legal, and social challenge.

India's legal response to computer-related offences was formally strengthened through the Information Technology Act, 2000, which established a statutory framework for electronic records and addressed several forms of computer misuse. Yet legal provisions alone do not ensure safe digital behaviour. Individuals must be able to recognize risks, evaluate suspicious online activity, protect credentials and personal information, and know how and where to report cyber incidents. For students, cybercrime awareness is therefore closely connected with digital literacy and responsible digital citizenship.

College students are an especially relevant population for cyber-awareness research because internet use is deeply embedded in academic, social, recreational, and financial activities. Frequent online activity can increase both competence and exposure. Students may know common terms such as hacking or viruses while remaining less familiar with phishing strategies, privacy settings, password hygiene, fraudulent links, malicious applications, reporting mechanisms, or legal remedies. Accordingly, cybercrime awareness should be conceptualized as a multidimensional construct involving knowledge of threats, preventive practices, and familiarity with appropriate responses.

Research conducted between 2000 and 2021 shows that awareness is not distributed uniformly across student populations. Studies have examined the influence of gender, academic discipline, educational level, security training, place of residence, and internet experience. Some studies report gender differences, while others find little or no meaningful difference once access and experience are considered. The present study contributes to this literature by examining college students in Rohtak district and comparing cybercrime awareness by gender and locality.

CONCEPTUAL BACKGROUND

Cybercrime and Cybersecurity Awareness

Cybercrime broadly refers to unlawful activities in which computers, digital devices, networks, or online systems function as a target, tool, or environment of the offence. Common student-relevant risks include phishing, account compromise, identity theft, malware, cyberstalking, social-engineering fraud, online financial scams, unauthorized access, and misuse of personal information. Cybersecurity awareness refers to an individual's knowledge and understanding of security threats together with the capacity to adopt safer practices. In educational settings, awareness is commonly assessed through knowledge of passwords, malware, phishing, privacy, safe browsing, and protective behaviour. Farooq, Isoaho, Virtanen, and Isoaho (2015) conceptualized information-security awareness among university students as a combination of knowledge and behaviour, emphasizing that merely feeling informed is not equivalent to demonstrating secure practices.

Cybercrime Awareness and the Student Population

Students are simultaneously beneficiaries of digital expansion and potential targets of cyber threats. Senthilkumar and Easwaramoorthy (2017), in a survey of college students in Tamil Nadu, examined awareness of threats such as viruses, phishing, password attacks, fake advertisements, and exposure of personal information. Their work demonstrated that student awareness is uneven across security domains and supported the need for systematic awareness programmes in higher education.

Alam, Qamar, and Husain (2018) examined cybercrime awareness and vulnerability among higher-education students and teachers in India and drew attention to gaps between general internet use and informed protective behaviour. Similarly, cyber-awareness initiatives among students in Delhi have emphasized that increased internet participation creates a need for preventive education concerning safe and healthy online practices.

Choudhary (2020) studied 500 higher-education students from Haryana using the CCAS-RS. The study reported average overall cybercrime awareness, higher awareness among professional-course students than traditional-course students, and no significant gender difference. This Haryana-based evidence is directly relevant to the present investigation because it suggests that educational exposure may be more consequential than gender.

Gender and Cybersecurity Awareness

Gender findings in cybersecurity research are mixed. Farooq et al. (2015), using 614 university students, reported significant gender differences in information-security knowledge and behaviour, with male students scoring higher on several dimensions. Their findings also suggested different learning preferences: male students relied more on self-exploration, whereas female students were more likely to use social networks and formal educational channels to acquire security knowledge.

By contrast, studies within Indian educational contexts have often found no significant gender difference. Choudhary (2020) reported comparable cybercrime awareness among male and female higher-education students in Haryana. Verma and Kushwaha (2021) also found that gender was not a significant indicator of cybercrime awareness among students in their educational sample. Kamalulail, Abdul Razak, Omar, and Mohamed Yusof (2021), studying university students in Malaysia, similarly found no significant gender difference in cybersecurity awareness.

The inconsistency across studies indicates that gender should not be treated as a direct or universal determinant of cyber-awareness. Differences may reflect field of study, computer experience, access to training, socialization, exposure to digital risks, or measurement methods. The current study therefore tests gender differences empirically rather than assuming that one gender is inherently more cyber-aware.

Locality, Digital Access, and the Rural-Urban Divide

Locality can influence cybercrime awareness through differences in digital infrastructure, frequency of internet use, availability of formal training, institutional resources, and exposure to online services. Rural and urban students increasingly use the same mobile platforms, yet their opportunities for structured digital education and cybersecurity guidance may differ.

Evidence from educational research suggests that place of residence can be associated with information-security awareness when it reflects broader differences in technology access and experience. Farooq et al. (2015) included area of living among individual factors relevant to student information-security awareness. In India, studies of cybercrime awareness have also examined locality as a demographic variable and have sometimes reported higher awareness in urban groups. Such findings are consistent with a digital-divide perspective in which awareness depends not merely on device ownership but on the quality, diversity, and educational context of digital engagement.

Need for the Present Study

The literature from 2000 to 2021 demonstrates the importance of examining cybercrime awareness within specific educational and socio-geographical contexts. Although studies have documented student vulnerability and varying levels of security knowledge, findings concerning gender remain inconsistent, and locality-related differences require further attention. The present study focuses on college students in Rohtak district and compares awareness by gender and by urban-rural locality. In doing so, it adds a localized empirical perspective to the broader literature on cybersecurity education and digital inequality.

Scope and Significance of the Study

The study is concerned with cybercrime awareness among college students and focuses specifically on differences associated with gender and locality. Cybercrime awareness includes familiarity with online threats and preventive knowledge relevant to common student activities such as social networking, digital communication, online transactions, and internet browsing.

The study is significant for educational institutions because cyber safety is now an essential component of student well-being. Awareness programmes can reduce vulnerability by helping

students identify suspicious communications, maintain strong passwords, protect personal information, respond to online harassment, and seek appropriate assistance. The results may also help colleges design interventions that are sensitive to disparities in digital access and prior exposure.

From a policy perspective, locality-based differences are important because digital inclusion should involve safe and informed participation, not merely internet connectivity. If rural students have lower awareness, cybersecurity education must be incorporated into wider digital-literacy initiatives so that expansion of digital access is accompanied by the knowledge required for safer use.

Objectives of the Study

1. To compare cybercrime awareness among male and female college students.
2. To compare cybercrime awareness among urban and rural college students.

Hypotheses

1. H01: There is no significant difference in cybercrime awareness between male and female college students.
2. H02: There is no significant difference in cybercrime awareness between urban and rural college students.

Methodology

The study employed a descriptive survey design. This design was appropriate because the purpose was to measure the existing level of cybercrime awareness and compare naturally occurring demographic groups without manipulating any variable.

Sample

The sample consisted of 100 college students from Rohtak district: 50 males and 50 females. The source study indicates the use of random sampling and also includes urban and rural subgroups. The reported analyses compare 50 urban and 50 rural students. Because the original wording of the subgroup composition is unclear, no additional cross-classification of gender by locality is assumed beyond the reported totals.

Tool Used

Cybercrime awareness was assessed using the Cyber Crime Awareness Scale (CCAS-RS) developed by S. Rajasekar (2013), the same instrument used in later Haryana research by Choudhary (2020). The scale is intended to assess knowledge and awareness concerning cybercrime and cyber-safety issues.

Statistical Techniques

Mean and standard deviation were used to summarize group scores. Independent-samples t tests were used to compare male versus female students and urban versus rural students. For a more scholarly interpretation of practical magnitude, Cohen's d was additionally calculated from the reported means and standard deviations. Statistical significance was evaluated at the .05 level.

RESULTS

The original numerical results have been retained. Exact p values shown below are approximate two-tailed values based on the reported t statistics with df = 98.

Table 1. Cybercrime Awareness by Gender

Gender	N	Mean	SD	t	Approx. p	Cohen's d	Decision
Male	50	141.42	25.15	1.8103	.073	0.19	H01 retained
Female	50	134.75	41.92				

Male students obtained a higher mean cybercrime-awareness score (M = 141.42, SD = 25.15) than female students (M = 134.75, SD = 41.92). However, the difference was not statistically significant, $t(98) = 1.81$, $p \approx .073$. The standardized mean difference was small ($d \approx 0.19$). Thus, the first null hypothesis was retained. The result indicates that the observed mean difference is insufficient to conclude that gender is a meaningful determinant of cybercrime awareness in this sample.

Table 2. Cybercrime Awareness by Locality

Locality	N	Mean	SD	t	Approx. p	Cohen's d	Decision
Urban	50	152.82	24.75	2.0902	.039	0.55	H02 rejected
Rural	50	140.51	19.76				

Urban students obtained a higher mean awareness score (M = 152.82, SD = 24.75) than rural students (M = 140.51, SD = 19.76). The difference was statistically significant, $t(98) = 2.09$, $p \approx .039$. The effect size was moderate ($d \approx 0.55$). Accordingly, the second null hypothesis was rejected. The result suggests that locality is associated with cybercrime awareness in the present sample.

DISCUSSION

The gender comparison showed no statistically significant difference in cybercrime awareness. Although males had a slightly higher mean score, the effect size was small. This finding is consistent with Choudhary's (2020) Haryana study, which also reported no significant gender difference among higher-education students. It is also compatible with Verma and Kushwaha (2021), who found gender not to be a significant indicator of cybercrime awareness, and with Kamalulail et al. (2021), who reported comparable cybersecurity-awareness levels among male and female university students.

The present result differs from Farooq et al. (2015), who found male university students to have higher information-security knowledge and behaviour. The contrast is instructive rather than contradictory. Different studies use different definitions and instruments: information-security awareness can include technical vocabulary, scenario-based behaviour, perceived competence, or broad cybercrime knowledge. Gender effects may therefore emerge in particular technical domains while disappearing when broader awareness is measured. Academic discipline and security training may also moderate gender differences.

The locality comparison revealed a statistically significant and moderately sized difference, with urban students scoring higher than rural students. This finding supports the view that cybercrime awareness is shaped by opportunity structures. Urban students may have greater exposure to broadband connectivity, formal computer education, digital banking, institutional cyber-safety initiatives, and diverse online services. Such exposure can create both greater risk and greater learning opportunities.

The locality finding should not be interpreted as evidence that rural students are intrinsically less capable of understanding cyber risks. Locality is likely to function as a proxy for multiple social and educational variables, including infrastructure, frequency and diversity of internet use, access to cyber-awareness programmes, institutional resources, and prior exposure to security incidents. A stronger research design would measure these factors directly.

The results reinforce a broader pattern visible in the 2000-2021 literature: cyber-awareness depends on knowledge, experience, and educational environment more than on a single demographic

characteristic. Senthilkumar and Easwaramoorthy (2017) showed that students may be aware of some threats while lacking knowledge in others. Choudhary (2020) found academic stream to be more influential than gender. These studies collectively support targeted educational interventions based on demonstrated knowledge gaps rather than assumptions about demographic groups.

The current findings also have an important methodological implication. The original manuscript described the significant rural-urban difference as supporting the second hypothesis, even though the stated second hypothesis was a null hypothesis of no difference. In the present scholarly rewrite, this has been corrected: the significant locality result requires rejection of H02.

Cybersecurity education should be integrated into college orientation and digital-literacy programmes rather than offered only after a cyber incident occurs.

Rural and less digitally resourced colleges may benefit from additional workshops on phishing, password security, privacy, social engineering, online fraud, cyberstalking, and incident reporting. Awareness interventions should be practical and behaviour-oriented, using simulated phishing examples, password-strength exercises, privacy-setting demonstrations, and case-based discussion.

Gender-neutral access to training is appropriate in view of the non-significant gender difference in the present study; however, programme design should remain sensitive to gender-specific experiences such as online harassment and cyberstalking. Institutions should publicize reporting pathways, cyber-cell contacts, and legal rights so that awareness includes both prevention and response. Digital inclusion policies should treat cybersecurity competence as part of meaningful digital access.

The sample was limited to 100 students from Rohtak district, which restricts generalization. The study used a cross-sectional descriptive design; causal explanations for locality differences cannot be established. The manuscript does not provide detailed demographic information such as academic stream, socioeconomic status, internet experience, device access, or prior cybersecurity training. The exact cross-classification of gender and locality is not clearly reported in the source manuscript. Cybercrime awareness was measured through a self-report scale; awareness scores may not perfectly predict actual cybersecurity behaviour. No reliability coefficient for the CCAS-RS within the present sample was reported. The study compares broad groups and does not examine specific domains such as phishing awareness, privacy behaviour, password practices, cyber-law knowledge, or reporting awareness.

The study demonstrates that cybercrime awareness among college students in Rohtak district is not significantly differentiated by gender, whereas locality is associated with a meaningful difference. Male and female students showed broadly comparable awareness, but urban students scored higher than rural students. In conjunction with research published between 2000 and 2021, the findings suggest that cybercrime awareness is shaped by digital exposure, educational opportunities, security knowledge, and access to cyber-safety resources. The practical response should therefore be educational rather than stereotypical: colleges should provide systematic, skill-oriented cybersecurity education for all students while directing additional resources toward groups and settings where access to cyber-awareness opportunities is comparatively limited.

REFERENCES

1. Alam, N., Qamar, O., & Husain, A. (2018). Cybercrime awareness, vulnerability and measures among higher education students and teachers: An exploratory study of India.
2. Choudhary, M. (2020). Cyber crime awareness among higher education students from Haryana with respect to various demographical variables. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(7), 14454-14461.
3. Farooq, A., Alifov, S., Virtanen, S., & Isoaho, J. (2018). Towards comprehensive information security awareness: A systematic classification of concerns among university students. Proceedings of the 32nd International BCS Human Computer Interaction Conference. https://doi.org/10.14236/ewic/hci2018.117
4. Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. In 2015 IEEE Trustcom/BigDataSE/ISPA (pp. 352-359). IEEE. https://doi.org/10.1109/Trustcom.2015.394
5. Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Observations on genderwise differences among university students in information security awareness. International Journal of Information Security and Privacy, 9(2), 60-74. https://doi.org/10.4018/IJISP.2015040104
Government of India. (2000). The Information Technology Act, 2000.
6. Kamalulail, A., Abdul Razak, N. E. N., Omar, S. A., & Mohamed Yusof, N. (2021). Awareness of cybersecurity: A case study in UiTM Negeri Sembilan Branch, Seremban Campus. e-Academia Journal, 11(1).
7. Meena, Y., Sankhla, M. S., Mohril, S., & Kumar, R. (2020). Cybercrime: Youth awareness survey in Delhi NCR, India. Forensic Research & Criminology International Journal, 8(5), 177-180.
8. Rajasekar, S. (2013). Cyber Crime Awareness Scale (CCAS-RS). [Scale used in the present study].
9. Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, 263, 042043. https://doi.org/10.1088/1757-899X/263/4/042043
10. Sridevi, K. V. (2020). Cyber security awareness among in-service secondary school teachers of Karnataka. Indian Journal of Educational Technology, 2(II), 82-94.
11. Verma, M. K., & Kushwaha, S. S. (2021). Awareness towards cybercrime among undergraduate students: The role of gender and college management. Shodh Sanchar Bulletin, 11(41), 116-121.