A Study of Awareness on Cybercrime among Students of Constituent Colleges of Cluster University Jammu

Dr. Mohd Zubair

Dean Faculty of Education Cluster University of Jammu-180016

DOI: https://doi.org/10.51584/IJRIAS.2026.11010093

Received: 20 January 2026; Accepted: 27 January 2026; Published: 11 February 2026

ABSTRACT

The rapid expansion of digital technologies and wide spread Internet use have significantly transformed contemporary life, particularly in the field of education. While cyberspace offers immense opportunities for learning, communication, and information sharing, it has also led to a sharp rise in cybercrime, exposing students to risks such as cyber fraud, identity theft, cyber bullying, and privacy violations. In this context, the present study investigates the level of cybercrime awareness among students of Constituent Colleges of Cluster University of Jammu. The study aims to assess overall awareness levels and examine differences in cybercrime awareness with respect to gender and area (urban and rural).

A descriptive survey method was employed, and a sample of 200 undergraduate students was selected through random sampling from five Constituent Government Colleges of Cluster University of Jammu. The Cybercrime Awareness Scale (CCAS) developed by Tibi et al. (2019) was used for data collection. Statistical techniques such as percentages, means, standard deviations, and the t-test were applied for data analysis.

The findings revealed that the majority of students possessed an average level of cybercrime awareness, while a smaller proportion demonstrated high awareness and a negligible number exhibited low awareness. A significant difference was found between male and female students, with female students showing higher cybercrime awareness. However, no significant difference was observed between students belonging to urban and rural areas.

The study highlights that although students demonstrate moderate awareness of cybercrime, there remains a need for systematic and structured awareness programmes. The findings underscore the importance of integrating cybercrime and cyber security education into higher education curricula to promote safe, responsible, and informed use of digital technologies among university students.

Key Words: Awareness, Cybercrime, Constituent Colleges, and Cluster University.

INTRODUCTION

The convergence of computer networks and telecommunication systems through digital technologies has led to the emergence of a shared virtual domain known as *cyberspace*. This cyberspace serves as a platform where diverse human activities increasingly converge through the Internet. In contemporary society, cyberspace has become one of the most dynamic and influential spaces, impacting nearly every aspect of human life. The Internet is extensively utilized for communication, commerce, advertising, banking, education, research, governance, and entertainment. There is scarcely any sphere of human activity that remains untouched by Internet technologies, making the digital environment an indispensable part of modern existence.

However, while the Internet has offered unprecedented opportunities and benefits, it has simultaneously introduced significant risks and challenges. Cyberspace has also become a hub for unlawful activities such as online pornography, gambling, human organ trafficking, drug trafficking, hacking, copyright infringement,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

cyber terrorism, privacy violations, money laundering, fraud, software piracy, and corporate espionage. The digital medium itself does not differentiate between lawful and unlawful conduct; rather, it merely facilitates human actions, irrespective of their ethical or legal nature.

Recognizing the need to regulate human behavior in cyberspace, the law has extended its domain into the digital world. In India, the idea of regulating electronic transactions was initially introduced through the E-Commerce Act, 1998. Subsequently, a comprehensive legal framework was established with the enactment of the Information Technology Act, 2000, which was later amended in 2008. The IT Act also introduced amendments to several existing statutes, including the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers' Books Evidence Act, 1891; and the Reserve Bank of India Act, 1934.

Despite the existence of this legal framework, the enforcement of cyber laws in India remains inadequate. A significant challenge lies in the limited technical understanding of cyber laws among law enforcement officials, lawyers, prosecutors, and judges, which hampers effective implementation. Moreover, cybercrime is not confined to national boundaries; it is a global phenomenon. Jurisdictional complexities further complicate cybercrime enforcement, as crimes can be committed in one country while being orchestrated or concealed in another. Similar to environmental regulation, cybercrime control requires international cooperation. Although international organizations such as the OECD and the G-8 have initiated discussions on collaborative mechanisms, disparities in legal priorities, cultural values, and socio-economic challenges among nations often provide cybercriminals with safe havens. Consequently, coordinated global efforts are essential to effectively address cybercrime.

Concept Of Cybercrime

Cybercrime, also referred to as computer crime, encompasses criminal activities that involve computers or computer networks either as the primary target or as a tool to facilitate unlawful acts. Such crimes include financial fraud, identity theft, trafficking in child pornography, intellectual property violations, and breaches of privacy. With computers becoming integral to commerce, governance, and entertainment, cybercrime has grown substantially in scope and significance.

Cybercrime can broadly be defined as any illegal activity in which a computer system, network, or digital device is involved. The United States Department of Justice categorizes cybercrime into three primary types:

a) **Hacker attacks**, where computers are used as weapons to disrupt or damage systems;
b) **Network penetration**, involving unauthorized access to computer networks or digital devices; and
c) **Computer-assisted crimes**, in which computers play a supporting role, such as storing illegally obtained data.

Financial gain remains the primary motivation for most cybercriminals. However, other factors such as ideological beliefs, personal revenge, the pursuit of notoriety, or recognition within hacker communities also contribute to cybercriminal behavior. By the 21st century, cybercrime had become a global phenomenon affecting even the most remote regions of the world. Warren Buffett has described cybercrime as one of the most significant challenges facing humanity, posing substantial risks to global security and economic stability. A McAfee-sponsored report (2014) estimated that cybercrime causes approximately USD 445 billion in annual losses to the global economy.

India, with over 560 million Internet users, ranks as the second-largest online market globally, following China. Projections indicate that this number is expected to exceed 650 million users. According to the National Crime Records Bureau (NCRB), 27,248 cybercrime cases were registered in India in 2018 alone, highlighting the growing magnitude of the problem.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Cybercrime poses a serious concern for educational institutions, particularly schools and colleges, as students are among the most active Internet users. The widespread use of social media platforms has provided cybercriminals with new avenues to exploit vulnerable users. The young individuals often disclose personal information online, engage with unknown individuals, and participate in unverified forums, thereby increasing their susceptibility to cyber threats. Such exposure not only affects individuals but also places families and institutions at risk.

Parents and educators play a crucial role in mitigating cyber risks by promoting awareness and monitoring online activities. Preventive strategies include establishing clear online usage guidelines, educating children about cyber security, promoting safe password practices, and encouraging responsible digital behavior. For individuals aged 18 to 25, who are heavily immersed in digital environments, targeted guidance is essential to help them recognize and manage online risks effectively.

Despite governmental initiatives aimed at strengthening cyber security infrastructure, awareness among college students remains at a moderate level, insufficient to counter evolving cyber threats. Hence, structured awareness programs and cyber security education must be integrated into higher education curricula to ensure safe and responsible use of cyberspace.

History Of Cybercrime

Although cybercrime does not have a singular point of origin, certain historical events are widely regarded as milestones in its evolution.

The earliest instance of cybercrime is often traced back to 1834, when two individuals infiltrated the French telegraph system to manipulate financial data. This incident is considered the first recorded cybercrime. With the invention of the telephone in 1876, new forms of technological exploitation emerged. By the late 19th century, unauthorized manipulation of telephone systems became prevalent, eventually evolving into “phreaking” during the mid-20th century.

An early example of ethical hacking occurred in 1940, when René Car mille, a French computer expert, sabotaged Nazi data-processing systems to prevent the registration of Jewish citizens. The rise of email communication in the 1980s and the advent of the Internet in the 1990s marked a significant turning point, as malware, phishing, and computer viruses became increasingly common.

The 21st century witnessed the proliferation of cybercrime through social media platforms, which enabled large-scale data theft and online fraud. More recently, the expansion of the Internet of Things (IoT) has created new vulnerabilities, allowing cybercriminals to exploit connected devices and cause damage that extends into the physical world.

Common Types Of Cybercrime

The dynamic and evolving nature of digital technology has contributed to the emergence of diverse forms of cybercrime. Common cybercrimes affecting students across age groups include:

i. **Cyber bullying**, which involves online harassment, stalking, doxing, and unauthorized access to social media accounts.
ii. **Cyber extortion**, including ransom ware attacks and online blackmail.
iii. **Cyber espionage**, involving unauthorized access to sensitive or classified information for political or economic gain.
iv. **Cyber stalking**, characterized by repeated online harassment intended to intimidate victims.
v. **Identity theft**, where personal information is misused for financial or legal fraud.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

vi. **Distribution of prohibited or illegal content**, including extremist material and child exploitation content.

Cybercrime Statistics

Recent data indicate a sharp increase in cybercrime-related losses worldwide. Annual financial losses from cybercrime have risen to approximately USD 6.9 billion. Business email compromise scams account for losses of USD 2.3 billion, while romance scams have caused losses nearing USD 953 million. Crypto currency-related crimes and technical support scams further contribute to financial damage. Although ransom ware losses appear comparatively lower, underreporting and indirect costs suggest a far greater economic impact than officially documented.

Global Cybercrime Awareness Status

Cybercrime has emerged as a major global security challenge, with cyber-attacks increasing at an unprecedented rate in recent years. Globally, cyber-attacks rose by approximately **125% in 2021** compared to 2020, and the upward trend continued throughout 2022, posing serious threats to both individuals and organizations. Among various forms of cybercrime, **phishing** continues to be the most prevalent and effective attack vector worldwide.

In 2021 alone, **323,972 Internet users** reported being victims of phishing attacks, indicating that nearly half of all data breach victims were compromised through phishing. During the peak of the COVID-19 pandemic, phishing incidents surged by **220%**, reflecting the increased reliance on digital platforms. Nearly **one billion email accounts were exposed in 2021**, affecting approximately **one in every five Internet users**, which further explains the persistence of phishing-related cybercrime.

Cybercrime has also resulted in significant financial losses globally. In 2022, the **average cost of a data breach for businesses was estimated at USD 4.35 million**. During the first half of the same year, approximately **236.1 million ransom ware attacks** were recorded worldwide. In the United States, **one in two Internet users** experienced account breaches in 2021, while **39 % of businesses in the United Kingdom** reported suffering cyber-attacks in 2022. Alarmingly, nearly **10% of U.S. organizations lacked cyber insurance**, increasing their vulnerability to digital threats.

Cybercrime affected approximately **53.35 million U.S. citizens** during the first half of 2022, while UK businesses incurred an average loss of **£4,200 per organization**. Malware attacks also escalated significantly, increasing by **358% in 2020** compared to 2019. Despite the evolving nature of cyber threats, phishing remains the most common and damaging cybercrime affecting individuals and businesses alike.

In terms of national cyber security preparedness, **Poland** ranks highest globally according to the **National Cyber Security Index (NCSI)**, which evaluates a country's ability to prevent and manage cyber incidents. As of December 2023, the top-performing countries included Poland (90.83), Estonia (85.83), Ukraine (80.83), Latvia (79.17), and the United Kingdom (75.00).

Region-wise analysis reveals that **Asian organizations suffered the highest proportion of cyber-attacks in 2021 (26 %)**, followed by Europe (24 **%**), North America (23 **%**), the Middle East and Africa (14 **%**), and Latin America (13 **%**Globally, cybercrime-related data breaches resulted in an average loss of **USD 787,671 per hour** in 2021. The United Kingdom recorded the highest number of cybercrime victims per million Internet users in 2022, at **4,783**, marking a **40% increase** compared to 2020 figures. The United States followed with **1,494 victims per million users**, though this represented a **13 % decrease** from 2020.

The UK and the USA have disproportionately high cybercrime victimization rates compared to other nations. In 2021, the USA recorded **759 % more victims** than Canada, the next highest country. Conversely, the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Netherlands experienced the largest increase in victims (50**%**), while **Greece reported the most significant decline**, with a 75 **%** reduction since 2020.

Globally, averages of 97 % data breach victims were **recorded every hour in 2021**. Between May 2020 and May 2021, cybercrime in the **Asia-Pacific region increased by 168 %**, with Japan alone experiencing a **40 % increase in cyber-attacks** in May 2021. Between the second and third quarters of 2022, countries such as China, Japan, and South Korea witnessed dramatic increases in data breaches, while Sri Lanka, Myanmar, and Iraq recorded significant declines. Overall, **108.9 million accounts were breached between July and September 2022**, equating to approximately **14 accounts compromised every second**.

A multinational case study conducted in 2022 revealed that **76 % of organizations** across the US, UK, Canada, Australia, and New Zealand experienced at least one cyber-attack during the year, compared to 55 **%** in 2020. Despite this, only **30 % of organizations had cyber insurance**, while **69% feared that a successful cyber-attack could force them out of business**, particularly among small and medium-sized enterprises.

The nature of cyber-attacks varies by region. In Asia and the Middle East, **server access attacks** were the most common, whereas **ransom ware dominated attacks in Europe, North America, and Latin America**. These patterns highlight the evolving and region-specific nature of cyber threats.

The growth of e-commerce and social media has further expanded the cybercrime landscape. Global e-commerce fraud is projected to cost the retail sector **USD 48 billion in 2023**, while online payment fraud is expected to result in losses of **USD 343 billion between 2023 and 2027**. Social media platforms have increasingly become targets of cybercrime, with Meta identifying over **400 malicious mobile applications in 2022** designed to steal Facebook login credentials. Cybercrime-related content violations remain widespread, as evidenced by Facebook removing millions of policy-violating posts related to bullying and harassment in 2022.

Cybercrime Awareness Status In India

India, like many other nations, has witnessed a rapid escalation in cybercrime incidents over the past decade. In 2018, approximately **208,456 cybercrime cases** were reported nationwide. Alarmingly, during just the first two months of 2022, **212,485 cybercrime cases** were reported surpassing the total number recorded in 2018.

The COVID-19 pandemic significantly accelerated cybercrime trends in India. Reported cybercrime cases increased from **394,499 in 2019** to **1,158,208 in 2020** and further to **1,402,809 in 2021**. Between the first and second quarters of 2022, cybercrime incidents increased by **15.3 %**, indicating a persistent upward trajectory.

Website hacking has also intensified in recent years. In 2018, approximately **17,560 Indian websites** were hacked, rising to **26,121 hacked websites in 2020**. Additionally, **78 %of Indian organizations** experienced ransom ware attacks in 2021, with **80 % of these attacks resulting in data encryption**, a rate significantly higher than the global average.

Financial fraud remains the most prevalent form of cybercrime in India, accounting for approximately **75 % of all reported cybercrime cases between 2020 and 2023**, with some years recording figures exceeding 77 **%**. The steady rise in cybercrime incidents highlights India's increasing exposure to digital vulnerabilities.

According to the **Norton Cybercrime Report (2011)**, nearly **30 million individuals in India** were victims of cybercrime, resulting in financial losses of approximately **USD 4 billion**. A key contributing factor to the widespread victimization is **cyber illiteracy**, underscoring the urgent need for comprehensive cyber awareness programs and digital literacy initiatives across all segments of society.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Cybercrime Awareness Status In Jammu And Kashmir (UT)

The Union Territory of Jammu and Kashmir has experienced a notable rise in cybercrime incidents in recent years. According to the National Crime Records Bureau (NCRB), cybercrime registrations in the UT increased by approximately **12% in 2022**, with **173 cases reported**, compared to **154 cases in 2021**. Although this increase is lower than the national average rise of **24 %**, a more pressing concern for Jammu and Kashmir is the **low charge-sheeting rate** in cybercrime cases.

The growing incidence of cybercrime presents a serious challenge that requires immediate and sustained intervention by law enforcement and administrative authorities. The high rate of dismissal or non-disposal of cybercrime charge sheets further aggravates the problem, weakening deterrence and public confidence in the justice delivery system. In comparison, larger states and other Union Territories have performed significantly better in meeting charge-sheet targets, highlighting a critical gap that the Jammu and Kashmir Police (JKP) must urgently address.

While it is acknowledged that the JKP faces multifaceted challenges including counter-terrorism operations and narcotics control the importance of prioritizing cybercrime investigations cannot be overstated. The exponential growth of cyber offenses necessitates a comprehensive and systematic response, emphasizing **public awareness, capacity building, and effective investigation mechanisms**. Authorities must initiate large-scale awareness campaigns to educate citizens about common cyber fraud techniques. Citizens, in turn, must remain vigilant, refrain from responding to suspicious communications, and promptly report any suspected cyber incidents. Strengthening investigative manpower and resources, along with fostering a culture of public awareness and timely reporting, is essential to effectively combat cybercrime in the UT.

Effects Of Cybercrime

Cybercrime has far-reaching consequences for individuals, organizations, and society at large. The major effects of cybercrime include:

a. **Decline in Share Value**: Cyber incidents often lead to loss of investor confidence, resulting in potential declines in a company's share price and overall market valuation.
b. **Capital Constraints**: Organizations affected by cyber breaches may face increased borrowing costs and challenges in raising capital.
c. **Regulatory Sanctions**: Breaches involving sensitive customer data may attract penalties, fines, or legal action from regulatory authorities.
d. **Reputational and Brand Damage**: Cyber-attacks erode customer trust, damage brand reputation, and can lead to loss of existing and prospective customers.
e. **Direct and Indirect Costs**: Cyber incidents result in substantial overheads, including increased insurance premiums, incident response costs, system remediation, legal services, and public relations expenditures.

Need For Cybercrime Awareness

One of the most significant technological advancements of the twentieth century is the invention and widespread adoption of the Internet. Today, more than half of the world's population actively uses the Internet across various domains such as communication, education, commerce, entertainment, and information dissemination. In education, the Internet has revolutionized learning through multimedia content, interactive resources, online communication, and access to vast repositories of information.

Visual and multimedia-based learning tools such as graphics, animations, videos, and documentaries have proven to be more effective than traditional text-based materials. Consequently, students increasingly rely on

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

digital platforms for academic engagement. Despite these advantages, the growing dependence on digital technologies has simultaneously increased exposure to cyber risks.

Given the prevalence of cybercrime, it is imperative to educate students about safe and responsible Internet usage. Cybercrime awareness enables learners to distinguish between beneficial and harmful online activities, thereby reducing vulnerability. This study seeks to contribute to such awareness by equipping students with the knowledge required to navigate the digital environment safely.

Cybercrime Prevention

1. Education and Training: Phishing and other cyber-attacks have become increasingly sophisticated, particularly in remote working environments. Regular training programs that educate users about evolving cyber threats are essential to enhance vigilance and reduce susceptibility.
2. Cyber Risk Management: Effective cyber security risk management requires a holistic approach involving all organizational units. Key actions include vendor risk assessment, identification of emerging threats, and implementation of internal controls, periodic testing of security systems and comprehensive documentation of risk mitigation efforts.
3. Cyber Defence Frameworks: The Cyber Defence Matrix, developed by Sounil Yu, provides a structured framework for understanding cyber security functions and aligning stakeholders to address cyber risks systematically.
4. Securing Mobile Devices: With increased reliance on smartphones and tablets, organizations must ensure mobile device security through regular updates, access control policies, zero-trust frameworks, and physical security measures.
5. Application Control: Organizations must monitor and regulate all applications used within their systems to minimize risks arising from shadow IT. Regular audits and enforcement of approved application policies are critical.
6. Security Policies and Enforcement: Comprehensive security policies such as password management, access control, and least-privilege policies must be implemented and strictly enforced to mitigate both internal and external cyber threats.

Government Initiatives To Tackle Cybercrimes

The Government of India has introduced multiple initiatives to address the growing cyber security challenges:

- **Indian Computer Emergency Response Team (CERT-In)**: Acts as the national nodal agency for incident response and cyber security management.
- **Cyber Surakshit Bharat**: Aims to enhance awareness and capacity building under the Digital India initiative.
- **Cyber Swachhta Kendra**: Focuses on detection and removal of malicious software and botnets.
- **National Cyber Security Policy**: Provides a framework for securing critical information infrastructure.

Additionally, the **Cyber security Centre of Excellence in Hyderabad**, established with support from the Telangana Government and the Data Security Council of India (DSCI), plays a pivotal role in innovation, start-up incubation, training, and policy support. These initiatives emphasize collaboration, research, capability building, and data protection to strengthen India's cyber security ecosystem.

Significance Of The Study

As India advances toward becoming a global digital hub, students across all age groups increasingly rely on ICT and Internet-based technologies. This heightened exposure makes them more vulnerable to cyber threats.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Lack of awareness can result in severe financial, emotional, and ethical consequences.

Cybercrime awareness equips students with knowledge of online risks, security practices, and emerging threats. Given the vulnerability of students especially in higher education the present study seeks to assess cybercrime awareness among undergraduate students in relation to **gender and location**. Understanding these variations provides valuable insights for targeted educational interventions. Hence, the researcher undertakes this study among undergraduate students in the **Jammu district of Jammu and Kashmir UT**.

Operational Definitions Of Terms

- **Cybercrime**: Any illegal activity carried out using computers, digital devices, or the Internet, including hacking, fraud, identity theft, and malware distribution.
- **Awareness**: The state of being informed, conscious, and knowledgeable about cybercrime and cyber security issues.
- **Students**: Students enrolled in undergraduate and professional programs under Cluster University of Jammu.
- **Constituent Colleges**: The five Constituent Colleges of Cluster University of Jammu.

Objectives Of The Study

1. To assess the level of cybercrime awareness among Students of Constituent Colleges of Cluster University Jammu.
2. To compare cybercrime awareness based on gender (male and female).
3. To compare cybercrime awareness based on area (urban and rural).

Hypotheses

1. There is no significant difference in cybercrime awareness among Students of Constituent Colleges of Cluster University Jammu based on gender.
2. There is no significant difference in cybercrime awareness among Students of Constituent Colleges of Cluster University Jammu based on area.

Delimitations Of The Study

- The study is confined to Students of Constituent Colleges of **Cluster University of Jammu** only.
- The sample size is limited to **200 students**.

Review Of Related Literature

The review of related literature plays a pivotal role in any research investigation, as it provides a comprehensive understanding of the problem under study and situates it within the broader academic context. It enables the researcher to identify research gaps, understand theoretical frameworks, select appropriate methodologies, and adopt suitable tools and statistical techniques for data analysis. A systematic review of existing studies also familiarizes the investigator with previous findings, trends, and scholarly debates relevant to the research problem.

A literature review involves a critical examination of books, research articles, reports, and other scholarly sources related to a specific area of inquiry. It not only summarizes key findings but also synthesizes existing knowledge to demonstrate how the present study contributes to and extends the existing body of research. In social science research, literature reviews are often organized thematically or conceptually, integrating both descriptive summaries and analytical interpretations. Such synthesis helps the researcher justify the need for

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

the present study and establish its academic significance.

Review Of Latest Indian Studies

Tejpal and Patole (2023) conducted a study titled *"Cyber security: Pressing Priority of India"*. The study highlighted a widening gap between the demand for cyber security professionals and the availability of skilled personnel in India. The researchers emphasized that low public awareness of cyber security practices significantly contributes to the rising incidence of cybercrimes, including hacking, phishing, and malware attacks.

Kaur and Bhatia (2023) examined *"Cybercrime and Cyber law Awareness among Youth"*. Their findings revealed that awareness of internet-related crimes, cyber laws, causes of cybercrime, and preventive strategies plays a crucial role in reducing cybercrime. The study stressed the importance of legal awareness in empowering youth to respond effectively to cyber threats.

Rajeswari and Ahmed (2022) investigated *"Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution"*. The study found that many students lacked adequate knowledge of data protection and privacy measures. Continuous exposure to digital platforms increased students' vulnerability to cyber threats, and the researchers recommended regular guidance and structured awareness programs.

Choudhuri (2022) conducted a study on *"Awareness among B.Ed. College Students towards Cybercrime"*. The findings indicated that students with limited knowledge of computers and internet technologies were more susceptible to cybercrime. The study emphasized the need to integrate cybercrime education into teacher education curricula to enhance awareness and preventive behavior.

Sahu and Shukla (2024) carried out a study titled *"Cybercrime Awareness among College Students"*. The study revealed that college students generally possessed above-average awareness of cybercrime. However, significant differences were observed based on locality, with urban students demonstrating higher awareness levels than rural students, while gender differences were found to be insignificant.

Review Of Latest Foreign Studies

Wu et al. (2023) conducted an extensive study on *"Research Trends in Cybercrime and cyber security"*. The study emphasized the need for holistic and interdisciplinary research approaches to understand the evolving nature of cybercrime. The researchers highlighted that mapping emerging trends helps scholars identify research gaps and fosters innovation in cyber security science.

Aphane (2023) explored *"cyber security Awareness on Cybercrime among Youth"*. The study revealed a critical lack of cyber security awareness among young people globally. Due to insufficient preventive knowledge, many youths were found to be inadequately prepared to identify and respond to cyber threats, increasing their vulnerability to online attacks.

Jalil et al. (2024) conducted a study titled *"cyber security Awareness among Secondary School Students Post-COVID-19 Pandemic"*. The research demonstrated that structured cyber awareness programs significantly enhanced students' cyber security knowledge and promoted safer internet usage. The study underscored the effectiveness of educational interventions in improving cyber safety.

Perwez et al. (2021) examined *"Cyber Security: An Exclusive Vagabond to Combat Cybercrime"*. The study highlighted that cyber security is essential for safeguarding data, networks, and information systems from

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

increasingly sophisticated cyber-attacks. The researchers emphasized the need for continuous technological upgrades and awareness initiatives to counter evolving cyber threats.

Sulaiman and Sreeya (2019) studied *"Public Awareness on Cybercrime with Special Reference to Age and Gender"*. Their findings revealed that cybercrime awareness varied significantly with age, whereas gender differences were not statistically significant. The study concluded that awareness programs should be tailored to different age groups for maximum effectiveness.

Linkage With The Present Study

The reviewed studies indicate that cybercrime awareness varies across demographic variables such as locality, educational exposure, and technological familiarity, while gender differences often remain inconclusive. Despite increasing digital penetration, awareness among students particularly in semi-urban and rural settings remains insufficient. These findings justify the need for the present study on **cybercrime awareness among Cluster University students in Jammu**, with specific reference to **gender and area**, to address regional and contextual research gaps.

RESEARCH METHODOLOGY

Research methodology refers to the systematic and logical framework through which a researcher plans and executes a research study in order to solve a defined research problem. It outlines the procedures, techniques, and strategies adopted to collect, analyze, and interpret data in a scientific manner. A well-structured research methodology ensures the reliability and validity of findings and enables the researcher to achieve the stated objectives of the study.

The methodology explains what type of data will be collected, the sources from which the data will be obtained, and the methods employed for data collection and analysis. It provides the research with scientific credibility and helps ensure that the conclusions drawn are based on sound evidence. Moreover, a clearly defined methodology allows readers to understand the approach adopted by the researcher and facilitates replication of the study by other researchers.

A sound research methodology offers several advantages. It provides a clear plan for conducting the research in a systematic manner, assists researchers in selecting appropriate tools and techniques aligned with the research objectives, and enables them to justify their approach when subjected to academic scrutiny. Additionally, it helps in documenting the intended outcomes of the research at the outset, ensuring consistency and direction throughout the investigation.

After identifying the research problem, it becomes essential to adopt appropriate procedures to achieve meaningful and accurate results. This chapter presents a detailed account of the methods and procedures employed in the present investigation. It includes information related to the research method used, population and sample, research tool, data collection procedure, administration of the tool, and the techniques used for data tabulation and analysis.

For the present study, the **descriptive survey method** was adopted to collect the required data. This method was considered appropriate as it enables the researcher to study and describe the existing status of cybercrime awareness among students.

Population And Sample

In research, the term *population* refers to the entire group of individuals or units that possess specific characteristics relevant to the study. It is often impractical for a researcher to collect data from the entire

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

population due to limitations of time, resources, and accessibility. Therefore, a representative subset of the population, known as a *sample*, is selected for investigation. The findings obtained from the sample are then generalized to the entire population.

Sampling is a crucial component of research methodology and forms the foundation of statistical analysis. The size and nature of the sample vary depending on the objectives and scope of the study. A well-chosen sample accurately reflects the characteristics of the population, thereby enhancing the validity and reliability of the research findings. Effective sampling saves time, effort, and cost while ensuring meaningful generalizations.

Population

The population of the present study consists of students studying in **five Government Colleges of Cluster University of Jammu**.

Sample

Out of the total five Government Colleges under the Cluster University of Jammu District, a sample of **200 students** was selected using the random sampling technique. The sample was equally distributed across **urban and rural areas**, comprising **100 students from urban colleges (50 males and 50 females)** and **100 students from rural colleges (50 males and 50 females)**. This balanced distribution was adopted to ensure adequate representation of gender and locality for comparative analysis in the present study.

Table-I Distribution of Sample

S.No	Name of the College	Number of Students			
		Male		Female	
		Urban	Rural	Urban	Rural
1.	Government PG College for Women, Gandhi Nagar	-	-	20	20
2.	Govt. Maulana Azad Memorial College Jammu	15	15	5	5
3.	Govt. SPMR College of Commerce	15	15	5	5
4.	Govt. Gandhi Memorial Science College	15	15	5	5
5.	Govt. College of Education	5	5	15	15
6.	**TOTAL=200**	**50**	**50**	**50**	**50**

Research Tool

Data for the present study were collected using appropriate research tools. A research tool refers to an instrument through which an investigator gathers required information from respondents. The proper selection of a suitable tool is essential for successful research.

For this study, a standardized questionnaire titled **Cybercrime Awareness Scale (CCAS)** developed by **Tibi et al. (2019)** was used. The scale consists of **23 positive statements** measured on a **five-point Likert scale**: Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, and Strongly Agree, with scores ranging from **1 to 5** respectively. The total score ranges from **23 to 115**, indicating very low to very high levels of cybercrime awareness.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Administration Of The Tool

The investigator personally visited the **five colleges under Cluster University of Jammu** to collect data. Permission was obtained from the Principals, and the purpose of the study was explained. The coordinators of digital initiatives were then approached and requested to respond to the questionnaire. Each respondent took approximately **15–20 minutes** to complete the scale. The filled questionnaires were collected immediately after completion.

Scoring Procedure

The Cybercrime Awareness Scale is a **self-administered and self-reporting tool**. Each item was scored from **1 to 5**, with higher scores indicating greater awareness. The total score was obtained by summing responses to all 23 items. Scores ranged from **23 (lowest awareness) to 115 (highest awareness)**. On average, respondents completed the scale within **10–15 minutes**.

Data Analysis And Interpretation

Data analysis refers to the systematic examination and processing of collected data in order to draw meaningful conclusions and enhance knowledge. It involves applying appropriate statistical and logical techniques to organize, summarize, and interpret data. According to Shamoo and Resnik (2003), analytical procedures help in drawing inferences by distinguishing meaningful information from random variations in data.

After data collection, the information must be properly organized and analyzed in accordance with the research plan. Raw data, by itself, does not reveal the true nature of the problem and therefore requires classification, tabulation, and summarization. Analysis involves breaking complex data into simpler components and rearranging them to identify patterns and relationships. Interpretation is the critical examination of analyzed data to derive valid conclusions.

Thus, even valid and reliable data becomes meaningful only when it is carefully and systematically analyzed and interpreted. This chapter presents the analysis of data followed by the interpretation of research findings in a systematic manner.

Table – II Level of awareness among Students of Constituent Colleges of Cluster University Jammu students about cybercrimes

Level of cybercrime awareness	**Number of students**	**Percentage**
High awareness	60	30.0%
Average awareness	135	67.5%
Low awareness	5	2.5%
	N= 200	

Table – II shows that out of 200 students, 60 (30.0%) students were having high level of cybercrime awareness, 135 (67.5%) students were having average level of cybercrime awareness, and 5 (2.5%) students were having low level of cybercrime awareness.

This distribution shows that the majority of students of Cluster University possess at least an average understanding of cybercrime, with relatively few at the low awareness level.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Table – III Level of awareness about cybercrimes among male and female students of Constituent Colleges of Cluster University Jammu

Category	High awareness	Average awareness	Low awareness
Male (N=100)	21 (21%)	76 (76%)	3 (3%)
Female(N=100)	39 (39%)	59 (59%)	2 (2%)

TABLE – III shows that out of 100 male students; 21(21%) students had high level of cybercrime awareness, 76(76%) students had an average level of cybercrime awareness, and 3 (3%) students had a low level of cybercrime awareness. In the case of 100 female students, 39 (39%) students had high level of cybercrime awareness, 59 (59%) students had an average level of cybercrime awareness, and 2(2%) students had a low level of cybercrime awareness. This suggests that while most students of both genders of Cluster University have average awareness, females seem to have slightly better awareness overall, with high percentage showing high-level awareness. These findings suggest that female students are more informed or cautious about online safety and digital threats.

Table – IV The significance difference between the level of awareness about cybercrimes among male and female students of Constituent Colleges of Cluster University of Jammu

Category	Sample size(N)	Mean	S.D	't'
Male	100	125.51	12.91	
Female	100	131.11	11.40	3.23

In Table-IV shows that the mean scores of 100 male and 100 female students were 125.51 and 131.11 and S.D were 12.9 and 11.40 respectively. The 't' ratio between the mean scores of male and female students comes out to be 3.23 which is significant at 0.01 level. It indicates that the male and female students differ significantly in their levels of awareness about cybercrimes. The female students were having better level of awareness about cybercrimes as compared to male students. Hence, hypothesis no. 1 **(There is no significant difference in Cybercrime awareness among Cluster University students on the basis of gender i.e., male and female)** is rejected.

Table – V Level of awareness about cybercrimes among students Constituent Colleges of Cluster University belonging to urban and rural areas

Category	High awareness	Average awareness	Low awareness
Urban (N=100)	32 (32.0%)	66 (66.0%)	2 (2.0%)
Rural (N=100)	28 (28.0%)	69 (69.0%)	3 (3.0%)

Table-V presents the distribution of cybercrime awareness levels among students of Cluster University from Urban and Rural areas. Among the 100 Urban students, 32(32.0%) had high cybercrime awareness, 66 (66.0%) had average cybercrime awareness, and 2 (2.0%) had low cybercrime awareness. In the case of 100 Rural students, 28 (28.0%) had high cybercrime awareness, 69 (69%) had average cybercrime awareness, and 3(3%) had low cybercrime awareness.

These findings show that students belonging from both the areas (urban and rural) of Cluster University show similar patterns, with majority having average cybercrime awareness and only a small number having low cybercrime awareness. However, urban students show a slightly better level of high cybercrime awareness. This could be due to better access to the internet, digital resources, and awareness programs in urban areas

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

compared to rural regions. Student of both the urban and rural areas show encouraging levels of cybercrime awareness.

Table –VI The significance difference between the level of awareness about cybercrimes among students of Cluster University belonging to urban and rural areas

Category	Sample size (N)	Mean	S.D	't'
Urban	100	126.67	12.56	
Rural	100	126.78	12.74	0.06

In Table VI shows that the mean scores of 100 urban and 100 rural students were 126.67 and 126.78 and S.D were 12.56 and 12.74 respectively. The't' ratio between the mean scores of urban and rural area students comes out to be 0.06 which is insignificant at 0.01 level. It indicates that the urban and rural area students do not differ in their level of awareness about cybercrimes. Hence, hypothesis No. 2 (There is no significant difference in Cybercrime awareness among Cluster University students on the basis of region i.e., rural and urban) is accepted.

THE EFFECT OF SIZES: Statistical significance alone does not indicate the magnitude of difference. Therefore, effect sizes were calculated using Cohen's d to determine the practical significance of the findings.

GENDER-WISE EFFECT SIZE: For gender differences;

- Male (M = 125.51, SD = 12.91, N = 100)
- Female (M = 131.11, SD = 11.40, N = 100)

Cohen's d = 0.46

This represents a moderate effect size, indicating that the observed gender difference is not only statistically significant but also educationally meaningful. Female students demonstrate a moderately higher level of cybercrime awareness than male students.

AREA-WISE EFFECT SIZE: For urban–rural comparison;

- Urban (M = 126.67, SD = 12.56, N = 100)
- Rural (M = 126.78, SD = 12.74, N = 100)

Cohen's d = 0.01

This reflects a negligible effect size, confirming that the difference between urban and rural students is practically insignificant, thereby strengthening the acceptance of the null hypothesis.

MAIN FINDINGS OF THE STUDY

The major findings of the study are summarized as follows:

1. The majority of students of Constituent Colleges of Cluster University of Jammu exhibited **average levels of cybercrime awareness**, while a smaller proportion demonstrated **high awareness**, and only a negligible percentage showed **low awareness**.
2. Both **male and female students** predominantly fell within the **average awareness category**, with female students showing a relatively higher proportion in the high awareness group.
3. Students from both **urban and rural areas** mostly possessed **average cybercrime awareness**, with very few students in either group exhibiting low awareness.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

4. Overall, cybercrime awareness among students was found to be **moderate**, with limited variation across **gender and locality**.

DISCUSSION OF RESULTS

The findings of the present study reveal that most undergraduate students of Cluster University of Jammu possess an **average level of cybercrime awareness**, which aligns with earlier studies by Rajeswari and Ahmed (2022) and Choudhuri (2022), who reported moderate awareness among higher education students. This suggests that while students are familiar with common cyber threats such as phishing and cyber fraud, their understanding may remain superficial.

The significant gender difference observed in the study, with female students demonstrating higher awareness, corroborates findings by Kaur and Bhatia (2023), who emphasized that female students tend to be more cautious and informed regarding online safety. However, these finding contrasts with studies such as Sulaiman and Sreeya (2019), where gender differences were insignificant, indicating that gender-based cyber awareness may be context-specific.

The absence of a significant difference between urban and rural students reflects increasing digital penetration and exposure across regions. This finding contradicts earlier studies (e.g., Sahu & Shukla, 2024) that reported higher awareness among urban students, suggesting that initiatives under Digital India may be gradually reducing the digital awareness gap.

EDUCATIONAL IMPLICATIONS

Based on the findings, the following educational implications are suggested:

1. Awareness programmes such as **workshops and webinars** should be organized regularly for students and teachers on emerging cybercrime issues.
2. **Technical training programmes** should be conducted for staff to promote safe and responsible use of digital technologies.
3. **Cyber security education** should be integrated into the higher education curriculum as a compulsory component.
4. Policies should be framed to educate young learners about cyber threats and preventive measures.
5. Regulatory bodies such as **UGC and MHRD** should take initiatives to reduce the **digital divide** between urban and rural students.
6. Cybercrime and cyber security literacy should be promoted **irrespective of gender and location**.
7. Credit-based **mandatory courses on cybercrime and cyber security** should be introduced at the higher education level.
8. Course content should be regularly updated to include recent cyber threats, malware, and online fraud practices.
9. Institutions should establish dedicated **cyber security committees** to oversee awareness activities and training programmes.
10. Periodic monitoring by national regulatory bodies should be ensured for effective implementation of cyber security initiatives.

LIMITATIONS OF THE STUDY

1. The study relied on self-reported data, which may be influenced by social desirability bias.
2. The CCAS total score was used without sub-dimensional analysis.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

SUGGESTIONS FOR FURTHER RESEARCH

The study suggests the following directions for future research:

1. Similar studies may be conducted in **other districts of the Union Territory** to enhance regional generalizability.
2. A **nationwide study** covering all states and Union Territories may provide comprehensive insights into cybercrime awareness.
3. Future research may examine cybercrime awareness at **school levels and across different higher education institutions**.
4. Cybercrime awareness among **especially abled learners** remains an under-researched area and requires focused investigation.

CONCLUSION

The present study concludes that undergraduate students of the Constituent Colleges of Cluster University of Jammu possess a **moderate level of cybercrime awareness**, with significant variation based on gender but not on locality. While digital access appears to be increasingly uniform across urban and rural areas, gaps persist in deeper cyber legal literacy and preventive preparedness. The findings emphasize the urgent need for structured, curriculum-integrated cybercrime education to promote responsible digital citizenship and resilience against evolving cyber threats.

REFERENCES

1. **Bhangla, A., & Tuli, J. (2022).** Analytical study on cybercrimes and its legal framework in India. International Journal of Law Management and Humanities, 4(2), 493–504.
2. **Choudhuri, S. K. (2022).** Awareness among B.Ed. college students towards cybercrimes. IOSR Journal of Humanities and Social Science, 27(11), 5–10.
3. **Philipose, G., & Karthik. (2022).** Assessing cybercrime awareness and internet usage among students. Journal of Hindustan Institute of Science and Technology, 11(11), 1147–1153.
4. **Raju, R., & Ahmed, A. (2022).** Cyber security awareness in using digital platforms among students in higher learning institutions. Journal of School of Computing and Information Systems, 16(8), 1124–1132.
5. **Tejpal, K., & Patole, J. (2023).** Cyber security: Pressing priority in India. Online Journal of Distance Education and E-Learning, 11(2), 2052–2061.
6. **Choudhary, M. (2020).** Cybercrime awareness among higher education students with respect to various demographic variables. Pal Arch's Journal of Archaeology, 17(7), 14454–14461.
7. **Shah, J. (2020).** Awareness about cyber laws for Indian youth. International Journal of Trend in Scientific Research and Development, 1(1), 10–16.
8. **Lakshmanan, A. (2019).** Cybercrimes and its preventive mechanisms. Journal of National Advanced Centre of Education and Research, 24(6), 1–5.
9. **Malhotra, T., & Malhotra, M. (2017).** Cybercrime awareness among teacher trainees. Scholarly Research Journal for Interdisciplinary Studies, 4(31), 5249–5259.
10. **National Center for Biotechnology Information (PMC). (n.d.).** Article on cyber security challenges — current and research-based (useful for literature background). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8579169/