IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

OPEN ACCESS

Volume: 4

Issue: 3

Month: July

Year: 2025

ISSN: 2583-7117

Published: 11.07.2025

Citation:

Dr. Jaya Sharma "Evaluating the Impact of Cybercrime Awareness: A Case Study" International Journal of Innovations in Science Engineering and Management, vol. 4, no. 3, 2025, pp. 59–65.

DOI:

10.69968/ijisem.2025v4i359-65

Evaluating the Impact of Cybercrime Awareness: A Case Study

Dr. Jaya Sharma[1]

[1]*Head, Deptt. of Computer Science College of Professional Studies, Ambikapur, Surguja, Chhattisgarh*

Abstract

An increasing number of internet users are exposing themselves to security risks when using the internet. As a result, it is possible to express worry over users' understanding of these problems and how safe and equipped they are to handle any eventuality. Review the many viewpoints on the effect of cybercrime awareness in this article. The review highlights the critical role of cybercrime awareness in reducing vulnerability and unlawful online behavior, particularly among youth. It finds a significant gap in understanding cyber laws, legal rights, and reporting mechanisms among internet users. Many perceive cybercrime as targeting only large entities, overlooking threats like phishing, cyberbullying, identity theft, and malware. The study also notes poor digital hygiene and complacency in updating security practices. Disparities exist in awareness across demographics. The conclusion emphasizes the urgent need for stronger awareness campaigns, legal enforcement, and collaboration among stakeholders to foster digital responsibility and enhance national cybercrime preparedness.

Keywords; Cybercrime Awareness, Cybercrime, Ransomware Attacks, Cyber-Attacks, Cybersecurity.

INTRODUCTION

The quick development of technology and the broad availability of the internet in today's linked globe have completely changed how people, organizations, and governments function. Despite the tremendous advantages of this digital revolution, there are also serious drawbacks, such as cybercrime. Cybercrime is the term used to describe a variety of illegal activities that are carried out through digital networks or the internet, with the intention of compromising users, data, and systems [1]. It encompasses a wide variety of offenses, including ransomware assaults, corporate espionage, and cyberterrorism, as well as common crimes like identity theft, online deception, and phishing schemes. It is imperative that society confront this critical issue, as the complexity and scope of cybercrimes continue to increase as technology advances. The extent of cybercrime is enormous and is growing [2]. Cybercrimes are more challenging to trace and prosecute than traditional offenses because they don't adhere to geographical boundaries. Because of the anonymity offered by the digital environment, criminals may target victims wherever they may be in the globe [3]. The effect of cybercrime is increased by its worldwide scope, which interferes with not only people's personal life but also with businesses' and governments' ability to operate. Cybercrimes have the potential to compromise sensitive data, cause billions of dollars in yearly financial losses, and undermine public confidence in digital networks [4]. Cybercrime has increased at an unprecedented rate in the digital era. The prospects for cybercriminals have increased due to the fact that over 5 billion people use the internet worldwide. Sophisticated cyber-attacks have been inadvertently facilitated by technological advancements, despite their beneficial nature [5]. For example, artificial intelligence and machine learning, which were first developed to boost productivity and creativity, are now being used as weapons to carry out automated assaults or produce phishing schemes that are very convincing [6]. A major increase in cybercrimes resulted from the COVID-19 pandemic's acceleration of digital reliance, which led to people and organizations depending more and more on online platforms for employment, education, and trade [7].

Cybersecurity awareness

The continuous process of teaching and training staff members on the dangers that exist in cyberspace, how to avoid them, and what to do in the case of a security crisis is known as cybersecurity awareness. Additionally, it helps them develop a proactive feeling of responsibility for maintaining the safety and security of the business and its assets. To put it simply, cybersecurity awareness is the ability to recognize security dangers and take appropriate action to reduce possible hazards [8].

Understanding cybersecurity best practices, the most recent security threats, the risks of downloading malicious attachments or clicking on harmful links, communicating online, sharing sensitive information, and other related topics are all part of cybersecurity awareness. By strengthening your company's security posture and streamlining its procedures, security awareness training programs help you create a more resilient enterprise. For cybersecurity awareness to be most successful and advantageous, it must be a company-wide endeavour [9].

Importance of cybercrime awareness

In order to safeguard your digital assets, cybersecurity awareness entails being aware of the many types of cyberthreats, being able to identify such dangers, and taking action to lessen their impact. Cybercrime and data theft cannot be completely eradicated just because you are aware of them. However, it does aid in avoiding the large losses that these assaults might cause to end users or enterprises. Therefore, in this era of the internet, cybersecurity awareness programs are essential for teaching people, kids, parents, and businesses about potential cyberattacks and how to avoid them [10].

The speed of information technology adoption is accelerating. As a result, more people are using the internet since it is now simple for everyone to access. Furthermore, technology is ever-changing and not static. End customers find it very difficult to understand the steps taken to safeguard their privacy. IT systems are essential to both individuals and businesses. However, they lack knowledge about cyber hazards, how to manage them, and how to safeguard themselves against them [11]. Educating individuals about potential cyberthreats and preventing data breaches are the main goals of a cyber-awareness program. Although there is no way to completely prevent assaults, there are ways to lessen their frequency and provide experts and end users useful information to assist them lower the dangers [12].

Importance of awareness and proactive measures

To enable people and organizations to defend themselves, awareness-building about cybercrime is crucial. By comprehending the diverse tactics employed by cybercriminals and the diverse categories of cyber threats, individuals can more effectively identify prospective hazards and respond accordingly [13]. A solid protection against cyberattacks requires proactive steps like choosing strong, one-of-a-kind passwords, turning on two-factor authentication, and updating software. Additionally, cultivating a cybersecurity-aware culture promotes ongoing learning and attentiveness, which lowers the likelihood of being a victim of cybercrime. Everyone has to be aware and proactive in protecting their digital life because as technology advances, so do the tactics used by cybercriminals [14].

Importance of cybercrime awareness programs

Programs to raise awareness of cybercrime are essential for reducing the hazards that come with a society that is becoming more and more digitalized. The nature of cyber threats, defense strategies, and safe online conduct best practices are all covered in these programs for communities, businesses, and people. The significance of awareness campaigns cannot be emphasized as cybercrime's frequency, complexity, and effect continue to rise [15].

1. Enhancing Individual Preparedness

Educating people on how to recognize and steer clear of such hazards is one of the main objectives of cybercrime awareness campaigns. Instead of technical deficiencies, numerous cybercrimes, including identity theft, phishing, and online schemes, capitalize on human vulnerabilities. Users can be instructed on how to identify deceptive emails, safeguard their credentials, and safeguard their personal information through awareness programs [16].

- **Real-World Impact:** According to studies, those who take part in cybersecurity training have a far lower chance of being infected with malware or falling prey to phishing scams. For example, by informing people about the dangers of oversharing information online, public awareness efforts like "Stop, Think, Connect" have shown promise in lowering cyber fraud instances.
- **Building Confidence:** Awareness programs not only decrease the probability of becoming a victim of cybercrime but also enhance the confidence and security of individuals in their digital interactions,

thereby encouraging increased participation in the digital economy.

2. Strengthening Organizational Security

Programs to raise awareness of cybercrime are essential for companies and organizations to avoid expensive breaches and interruptions. The effectiveness of a security solution may be determined by the activities of employees, who are often the first line of defense against cyber-attacks [17].

- **Reducing Insider Threats:** A lot of cyber issues are caused by workers making unintentional errors, such using weak passwords or clicking on harmful websites. According to The Global Risk Report (2020), awareness training is instrumental in mitigating these risks by providing employees with information regarding "secure practices and the potential repercussions" of their actions.
- **Compliance with Regulations:** Regulations like the CCPA, GDPR, and HIPAA, which are strict cybersecurity laws, apply to many businesses. Employee comprehension and adherence to security procedures are ensured by awareness programs, which assist firms in meeting compliance standards.
- **Economic Benefits:** Recovering from an assault is significantly more expensive than preventing cybercrime via knowledge. Financial losses, reputational injury, and legal penalties can be prevented by businesses that mitigate the risk of breaches.

3. Addressing Psychological and Social Impacts

Awareness campaigns include the psychological and social aspects of cybercrime in addition to technical information. People who are victims of fraud, harassment, or cyberbullying often experience anxiety, emotional discomfort, and a decline in faith in digital systems.

- **Empowering Vulnerable Groups:** Those most at risk may get customized counsel from programs designed for certain populations, such as children, the elderly, and small business owners. Young people may avoid cyberbullying and safeguard their digital identities by being taught about the risks of disclosing personal information online.
- **Promoting Digital Responsibility:** In addition, awareness campaigns promote ethical online conduct, thereby cultivating a culture of accountability and respect in digital interactions. By doing this, hate speech and cyberbullying may be less common.

4. Supporting National and Global Security

By lowering vulnerabilities across sectors, cybercrime awareness initiatives are essential to enhancing both national and international security (NIST, 2022). Critical infrastructure, including financial institutions, healthcare systems, and electricity grids, may be severely impacted by cyberattacks [12].

- **Public-Private Collaboration:** To guarantee wide reach, governments and commercial organizations often work together on awareness campaigns. All facets of society are made more aware of cyberthreats, for example, via initiatives like European Cybersecurity Month.
- **Creating a Cyber-Resilient Society:** By reducing harm and guaranteeing continuity, awareness campaigns help create a society that is cyber-resilient, where people and institutions are prepared to react to threats in an efficient manner.

5. Fostering International Cooperation

Programs to raise awareness also encourage international cooperation since cybercrime is a worldwide problem. In order to address cross-border cyber hazards, countries can collaborate by exchanging resources, knowledge, and best practices.

- **Unified Efforts:** The importance of education and awareness in avoiding cybercrime globally is highlighted by initiatives such as "the Budapest Convention on Cybercrime". Campaigns that operate together may tackle cross-border problems including ransomware, phishing networks, and online fraud.

6. Preparing for Future Challenges

Because technology is developing at such a fast rate, cyber-crime is always changing. In order to mitigate emerging threats, including AI-driven attacks, quantum computing vulnerabilities, and deepfakes, awareness programs must remain in sync with these developments.

- **Encouraging Lifelong Learning:** Raising awareness of cybersecurity shouldn't be a one-time event. In the face of new risks, ongoing education

guarantees that people and organizations stay alert and flexible.

- **Inspiring Innovation:** Raising awareness of the worldwide lack of qualified workers in cybersecurity might also encourage people to seek employment in the industry.

LITERATURE REVIEW

(Pandey & Kapoor, 2025) [18] This essay examines the many ways that cybercrime affects society, from identity theft and breaches of personal data to massive corporate and governmental assaults that endanger national security and economic stability. It goes deeper into people's and organizations' awareness levels, pointing out the gaps that leave them vulnerable to cyberattacks. Artificial intelligence and machine learning, two technological developments in cybersecurity, are highlighted as essential instruments to anticipate and lessen these risks. In order to increase digital literacy, the publication also promotes extensive educational programs that emphasize safe online conduct and preventative measures. The goal of the study is to address these aspects and promote trust and resilience in the constantly interconnected global community in order to help create a safer digital environment.

(Alhadidi et al., 2024) [19] This essay offers a thorough examination, combining theoretical and empirical viewpoints, of how legal awareness and cybercrime affect young people's conduct in society. Using a questionnaire given to a population consisting of a random sample of 2000 students registered at the University of Jordan, the focus of our case study, a quantitative inquiry was conducted to address the issue at hand. Our study's results show a strong and unquestionable correlation between students' involvement in illegal cyber-acts and their level of legal understanding of cyber criminality. Furthermore, the results show that gender and a number of other characteristics have an impact in deterring students from committing such crimes. As a result, this emphasizes how important it is to put into practice efficient methods to raise students' legal knowledge of cybercrime in order to reduce their participation.

(Datt, 2024) [20] The main goal of the study is to evaluate young people in India's awareness of cybercrime and how it affects their level of life satisfaction. The link between the aforementioned factors was investigated and understood using a cross-sectional design. The statistical method used to determine and comprehend the link between life happiness and cybercrime awareness was correlational analysis, and the results showed a negative correlation between the two variables. Furthermore, the standard deviation implies that respondents' life satisfaction scores and awareness of cybercrime are somewhat variable. The model did not provide a substantial fit, as shown by the Regression Analysis, another statistical method used in this investigation. Consequently, Cybercrime Awareness did not account for any variance in life satisfaction. The study's applications and limitations have also been discussed.

(K & V K, 2024) [21] Consequently, each nation, including India, is experiencing a significant rise in cybercrime. Since digital technology is always evolving, cybercrime faces its greatest challenge: it is dynamic. The danger of cybercrime is growing along with the digital environment. The foundation of India's legislative framework for preventing cybercrime and advancing cyber security is "the Information Technology Act of 2000". By implementing a combination of technological advancements, public awareness, and robust legislation, India can effectively combat cybercrime and create a secure digital environment for its citizens. Because of this, there are a lot of different ways that cybercrime is committed, and in order to stay up with the always changing dangers, it is crucial that cyber laws be updated and strengthened.

(Sani et al., 2024) [22] Examining youth knowledge of cybercrime in Kaduna State, Nigeria's "Kaduna South Local Government Area (KSLGA)" was the aim of this research. Primary data was gathered via an in-depth interview and a semi-structured questionnaire. Descriptive statistical approaches were used to examine and report the acquired data. According to the findings, 83 percent of the young people polled knew about the many types of cyberthreats. In addition, the poll revealed that young men exhibit more awareness than young women. To sum up, the research offers suggestions for raising youth awareness of cybercrime in KSLGA and worldwide.

(Bundela & Kumari, 2021) [23] The modern era is characterized by an addiction to the internet and computers, as we all reside in the era of "Information and Communication Technology (ICT)". We cannot dispute the significance of the internet in our daily lives. Computers and the internet play an essential role in society. We were able to comprehend how quick, easy, and efficient everything was. The teaching and learning process is enhanced by the internet. The paper cites online tutoring and online learning as two examples. "A Study of Cyber Crime Awareness among College Students" is the subject that the investigator has chosen. It will include the investigator gathering data on

college students' awareness of cybercrimes and assessing their knowledge of these kinds of crimes. Thus, the aforementioned subject is crucial for college students.

(Mali et al., 2018) [24] This essay has offered an overview of current perspectives on the difficulties posed by cybercrime. First, the definitions of cybercrime and cyberwarfare were found to be lacking in consensus. The results of the study of 325 users are presented to assess their perceptions of security issues, their cognizance, and their attitudes toward the use of related software. Despite the fact that respondents claim to be aware of the risks and to have used many of the crucial safeguards, the results show that there are some areas where basic knowledge and understanding are lacking. Users who considered themselves to have advanced levels of online expertise also showed remarkable ignorance, despite the fact that a significant percentage of the problems were usually severe among novice users.

(Mathias & B, 2018) [25] Through the use of a questionnaire and analysis of the data, this research seeks to determine the degree of awareness regarding "cybercrime and cyber security" across postgraduate and undergraduate students at government universities. To complete the survey, 250 students in the 17–21 age range were chosen at random. Therefore, on October 17, 2018, a seminar for college students was held with the title "CYBER CRIME- Latest trends and challenges - its detection, investigation and conviction (Cyber legal challenges)". Among the 185 participants, 120 provided comments. They thought the presentation was pertinent and helpful. The cause will undoubtedly benefit from more programs of this kind or from their inclusion in the academic curriculum.

(Chanuvai Narahari & Shah, 2016) [26] It is getting more difficult to protect netizens from cybercrimes as a result of India's growing internet usage and convergence with digitally enabled platforms and devices. The harsh fact is that, despite the rapid advancements in internet-enabled tools and applications, internet consumers are not being informed about security vulnerabilities and dangers. Consequently, "the current research paper" is dedicated to determining the answers to the following alarming questions: "Is the netizen truly cognizant of their vulnerability to a variety of cyber-crimes?", "To what extent is the netizen cognizant of their vulnerability?", and "If the netizen is not cognizant of cybercrimes, what strategies can be implemented to increase their awareness and awareness?" The study proposed a conceptual framework that explains how to maintain and carry out awareness campaigns on cybercrimes among internet users.

RESEARCH GAP

Despite growing global efforts to enhance cybercrime awareness, existing literature lacks a comprehensive evaluation of its actual impact on user behavior, cybersecurity practices, and crime prevention effectiveness. Most studies focus on awareness campaigns or general knowledge dissemination, without assessing their long-term influence on reducing cyber threats or improving digital resilience. Furthermore, there is limited research that compares the effectiveness of various awareness strategies across different demographics, regions, and platforms. This gap highlights the need for a systematic review to evaluate the measurable outcomes of cybercrime awareness initiatives and identify best practices for designing impactful awareness programs.

RESEARCH OBJECTIVE

- In this article study the various literature’s research on cybercrime awareness.
- Study the Importance of cybercrime awareness and cybercrime awareness programs.

RESEARCH METHODOLOGY

This review paper adopts a qualitative research methodology, utilizing secondary data to evaluate the impact of cybercrime awareness on individuals and organizations. The study is grounded in an extensive literature review, systematically analyzing peer-reviewed academic journals, scholarly articles, government reports, technical papers, and case studies published between 2016 and 2025. The focus is on identifying trends, patterns, and outcomes related to cybercrime awareness initiatives, including educational campaigns, training programs, and digital literacy efforts. By critically assessing existing literature, the study aims to understand the effectiveness of awareness strategies in enhancing cybersecurity behavior and reducing vulnerability to cyber threats.

CONCLUSION

The findings of this review paper highlight the critical role of cybercrime awareness in preventing unlawful digital activities and reducing vulnerability among individuals, particularly students and young internet users. While increased awareness has shown a positive impact on understanding cybercrime and associated legislation, the effectiveness remains limited due to several factors. A significant gap exists in legal enforcement, with only a few

cybercriminals facing prosecution, and victims often unaware of their legal rights or reluctant to take legal action. Many individuals mistakenly perceive cybercrime as targeting only large institutions, overlooking the risks posed to everyday users. Crimes such as cyberstalking, phishing, identity theft, cyberbullying, and illegal content sharing remain poorly understood. The study also found that users often neglect basic digital hygiene practices, including password security and antivirus updates, making them more susceptible to attacks. While some segments of society demonstrate a proactive approach to cybersecurity, others lack awareness and access to protective resources. The study concludes that to effectively combat cybercrime, a multi-faceted approach is required, including stronger legal frameworks, enhanced public awareness campaigns, improved reporting mechanisms, and international cooperation. The Information Technology Act, 2000 in India must be enforced rigorously, with increased government initiatives to educate and empower users across all demographics.

REFERENCES

[1] P. Punia, Sunita, and M. Phor, "Study of Cyber Crime Awareness in Relation to Internet Addiction," *Learn. Community*, vol. 10, no. 1, pp. 29–40, 2019, [Online]. Available: https://www.indianjournals.com/ijor.aspx?target=ijor:lco&volume=10&issue=1&article=004

[2] G. Das, Y. A. Ali, M. B. Singh, and M. K. Nag, "Digital Forensics in E-Commerce: Investigating Online Payment Fraud and Data Breaches," *Int. J. Innov. Sci. Eng. Manag.*, vol. 4, no. 1, 2025, doi: 10.69968/ijisem.2025v4i1262-268.

[3] S. I. Alsharif, W. Al-Qahtani, A. Alotaibi, L. Al-Subaie, and M. Melhem, "The impact of cybercrime and social media on intellectual security and awareness with University students in KSA: a field study on students of Imam Abdulrahman Bin Faisal University," *Cogent Arts Humanit.*, vol. 11, no. 1, p., 2024, doi: 10.1080/23311983.2024.2312662.

[4] A. Sayyad, R. Dusane, A. Hanamghar, S. Bhoite, and D. B. J. Mohite, "A STUDY ON AWARENESS ABOUT CYBER- CRIME AMONG COLLEGE STUDENTS," *Int. J. Nov. Res. Dev.*, vol. 8, no. 10, pp. 356–362, 2023.

[5] Y. K and S. K. C. R, "A Study on Cyber Crime Awareness among B. Ed Teacher Trainees," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 11, pp. 2103–2110, 2023, doi: 10.22214/ijraset.2023.57014.

[6] M. P. Gupta and P. (Dr. . L. Singh, "The Rising Threat of Recruitment Frauds – Analysing the Role of HRM Practices in Mitigating Cybercrime in India," *Int. J. Innov. Sci. Eng. Manag.*, vol. 4, no. 1, 2025, doi: 10.69968/ijisem.2025v4si194-102.

[7] W. T. Gandela, L. D. Damiar, and R. M. Pajo, "CYBERCRIME AWARENESS AMONG DORSU-CEC STUDENTS IN CATEEL, DAVAO ORIENTAL," *IJARIIE*, vol. 10, no. 5, pp. 1067–1088, 2024.

[8] B. Dupont, F. Fortin, and R. Leukfeldt, "Broadening our understanding of cybercrime and its evolution," *J. Crime Justice*, vol. 47, no. 4, pp. 435–439, 2024, doi: 10.1080/0735648X.2024.2323872.

[9] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data Cogntive Comput.*, vol. 5, no. 23, pp. 1–15, 2021.

[10] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Pap. Risk Insur. - Issues Pract.*, vol. 47, no. 3, pp. 698–736, 2022, doi: 10.1057/s41288-022-00266-6.

[11] M. Anant, K. Kanwar, and S. KumarIndulkar, "An Empirical Study On Awareness Of Cyber Security In Digital Banking Among College Going Students (With Special Reference To Korba District Of Chhattisgarh)," *Int. J. Innov. Sci. Eng. Manag.*, vol. 3, no. Specail, pp. 45–49, 2024.

[12] I. K. Azzani, S. Adi Purwantoro, and H. Zakky Almubarok, "Enhancing awareness of cyber crime: A crucial element in confronting the challenges of hybrid warfare in Indonesia," *Def. Secur. Stud.*, vol. 5, no. 1, pp. 1–9, 2024, doi: 10.37868/dss.v5.id255.

[13] A. Singh and N. Shanker, "Redefining Cybercrimes in light of Artificial Intelligence : Emerging threats and Challenges," pp. 192–201, 2024, doi: 10.69968/ijisem.2024v3si2192-201.

[14] D. G. Philipose and M. K. A, "Assessing Cybercrime Awareness and Internet Usage among Students: Implications for Policy and Education," *Eur. Chem. Bull.*, vol. 11, no. 11, 2022, [Online]. Available: file:///C:/Users/SOPHIA MACHEMBA/Downloads/40a501653e69b45c421d2435f9c6a497 (1).pdf

[15] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, vol. 7, no. 1, p. e06016, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[16] M. Ahmead, N. El Sharif, and I. Abuiram, "Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study," *Crime Sci.*, vol. 13, 2024, doi: 10.1186/s40163-024-00230-w.

[17] V. K. Viraja and P. Purandare, "A Qualitative Research on the Impact and Challenges of Cybercrimes," *J. Phys. Conf. Ser.*, vol. 1964, no. 4, 2021, doi: 10.1088/1742-6596/1964/4/042004.

[18] P. Pandey and A. Kapoor, "Cybercrime in the Digital Era: Impacts, Awareness, and Strategic Solutions for a Secure Future," *Sachetas*, vol. 4, no. 1, pp. 32–37, 2025, doi: 10.55955/410004.

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

[20] S. S. Datt, "Assessing Cybercrime Awareness among Indian Young Adults and its Impact on their Satisfaction with Life," *Int. J. Indian Psychol.*, vol. 12, no. 2, 2024, doi: 10.25215/1202.128.

[21] N. K and C. V K, "A Study On Cybercrime Its Impact And Awareness Towards Society," *Int. J. Creat. Res. Thoughts*, vol. 12, no. 4, pp. 23–31, 2024.

[22] K. M. Sani *et al.*, "Study on Cybercrime Awareness Among Youths in Kaduna South Local Government Area, Kaduna State, Nigeria," *Int. J. Indian Psychol.*, vol. 12, no. 4, 2024, doi: 10.25215/1204.006.

[23] S. Bundela and K. Kumari, "A STUDY OF CYBER CRIME AWARENESS AMONG COLLEGE STUDENTS," *Psychol. Educ.*, vol. 58, no. 2, pp. 8861–8865, 2021.

[24] P. Mali, J. S. Sodhi, T. Singh, and S. Bansal, "Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: An empirical study," *Int. J. Mech. Eng. Technol.*, vol. 9, no. 2, 2018.

[25] D. A. P. Mathias and S. B, "a Survey Report on Cybercrime Awareness Among Graduate and Postgraduate Students of Government Institutions in Chickmagaluru, Karnataka, India and a Subsequent Effort To Educate Them Through a Seminar," *Int. J. Adv. Res. Eng. Technol.*, vol. 9, no. 6, pp. 214–228, 2018.

[26] A. Chanuvai Narahari and V. Shah, "Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India)," *Ijariie*, vol. 2, no. 6, pp. 2395–4396, 2016.