

# CYBERCRIME AWARENESS, PRACTICES, AND REPORTING BEHAVIOR: AN EMPIRICAL STUDY IN RAJASTHAN

Deepak Kumar Parewa<sup>1</sup>, Dr Deepa Mordia<sup>2</sup>

<sup>1</sup>Research scholar, Department of Statistics, University of Rajasthan, Jaipur, Rajasthan, India

<sup>2</sup>Assistant Professor, Department of Statistics, University of Rajasthan, Jaipur, Rajasthan, India

\*\*\*

**Abstract:** *The increasing reliance on digital technologies has created both opportunities and risks in India. Rajasthan, with its rapidly expanding internet penetration, has seen a rise in cybercrimes that challenge individuals, institutions, and government systems. This study investigates cybercrime awareness, online safety practices, and reporting behavior among 392 respondents (171 male and 221 female). Data was collected using a structured questionnaire and analyzed with descriptive statistics, chi-square tests, factor analysis, independent samples t-tests, and regression models. Results reveal that although respondents are aware of basic cybercrimes like scams and hacking, knowledge about phishing, ransomware, and identity theft is relatively low. While safe practices such as using strong passwords and avoiding suspicious links are common, the adoption of advanced safety measures such as two-factor authentication and regular system updates is limited. Gender and education differences were observed, with men demonstrating higher cyber hygiene and threat literacy, while women showed greater readiness to report incidents. Regression analysis confirmed that cybercrime response behavior is the strongest predictor of reporting readiness. These findings contribute to statistical literature and have important policy implications for awareness campaigns, digital literacy programs, and the development of victim-friendly reporting mechanisms.*

**Key Words:** Cybercrime, Awareness, Reporting Behavior, Rajasthan, Cyber Hygiene and Digital Literacy

## 1. INTRODUCTION:

The digital revolution has transformed societies worldwide, enabling unprecedented connectivity, access to information, and economic opportunities. However, this progress has also introduced significant vulnerabilities, especially in the form of cybercrime. Cybercrime refers to illegal activities conducted through digital means, including fraud, hacking, identity theft, ransomware, and online harassment. According to the National Crime Records Bureau (NCRB, 2022), cybercrime incidents in India have increased more than fourfold in the past decade, with financial frauds and data breaches being the most common. These crimes not only lead to financial losses but also undermine trust in digital platforms and hinder the adoption of digital services.

Rajasthan, one of the largest states in India, has experienced rapid growth in internet usage due to expanding mobile penetration and government initiatives such as *Digital India*. With a diverse demographic profile comprising both urban and rural populations, the state provides a unique setting to examine awareness and practices related to cybercrime. Despite government campaigns, awareness levels remain uneven, and many victims fail to report cybercrimes due to fear of legal processes, lack of knowledge, or social stigma. This context makes Rajasthan an important case study for understanding cybercrime from a statistical and behavioral perspective.

Existing literature highlights three main concerns: (a) although general awareness of cybercrime is increasing, specific knowledge about sophisticated threats such as phishing and ransomware remains low; (b) while individuals report using safe practices such as strong passwords, compliance with advanced safeguards like two-factor authentication is weaker; and (c) there exists a large gap between victimization and reporting, suggesting trust and institutional barriers. These issues raise critical questions for researchers and policymakers alike.

From a statistical perspective, analyzing primary data on awareness, practices, and reporting behavior provides valuable insights into the distribution of digital literacy and cyber readiness across demographic groups. Tools such as chi-square tests, factor analysis, t-tests, and regression allow for testing hypotheses regarding gender and education differences, as well as identifying predictors of reporting readiness. Such analysis contributes not only to academic literature in statistics and criminology but also offers practical implications for designing targeted interventions.

This study focuses on cybercrime in Rajasthan with three key motivations. First, cybercrime cases in the state have been rising steadily, yet systematic research using primary data remains scarce. Second, demographic factors such as gender

and education are expected to play an important role in shaping cyber awareness and practices, but empirical evidence is limited. Third, reporting behavior is a critical dimension, as awareness alone does not ensure safety unless individuals are willing and able to seek legal remedies. By addressing these concerns, the present study bridges the research gap and provides both statistical and policy-oriented contributions.

The remainder of this paper is organized as follows. Section 2 reviews existing literature and theoretical frameworks on cybercrime awareness and practices. Section 3 outlines the objectives and hypotheses of the study. Section 4 details the research methodology, including data collection and statistical tools. Section 5 presents the results of descriptive and inferential analysis, supported by tables and graphs. Section 6 discusses findings in the context of previous research and theories. Finally, Section 7 concludes with policy implications, limitations, and directions for future research.

## 2. REVIEW OF LITERATURE

The rapid advancement of information and communication technologies (ICT) has drawn considerable academic attention toward cybercrime and its socio-technical implications. Scholars across the globe have examined awareness levels, preventive practices, and the psychological as well as social determinants of reporting behavior. This section reviews international and Indian studies while highlighting theoretical frameworks that guide the present research.

### International Studies

- Livingstone and Helsper (2007) analyzed digital inclusion among children and young people in the United Kingdom and demonstrated that access does not guarantee safety. Their findings emphasized that even frequent internet users are vulnerable if awareness of risks is incomplete. Similarly, Williams (2006) examined cybercrime victimization in the United States and observed that identity theft and online fraud were the most commonly experienced crimes, with reporting rates remaining low due to fear of reputation loss. In another influential study, Holt and Bossler (2008) applied Routine Activity Theory to cybercrime and found that individuals with high internet exposure but weak protective measures were more likely to be victimized.
- Horan, C., & Saiedian, H. (2021) focused on digital forensics and open-source intelligence as the main categories of cyber investigations, comparing various tools and methods used by investigators. It establishes criteria for evaluating the effectiveness and applicability of these tools. The findings reveal that no single tool can gather all necessary evidence, requiring a combination of tools for effective investigations. In mobile digital forensics, logical extraction and hex dumps are identified as the most effective and least damaging methods. In open-source intelligence, natural language processing is highlighted as the most versatile and useful tool. This comparison underscores the importance of using a multifaceted approach in cyber investigations.
- In East Asian contexts, Lee (2015) studied South Korean university students and concluded that while awareness about cyberbullying was high, adoption of preventive practices such as privacy settings remained inconsistent. Yeboah-Boateng and Amanor (2014) explored Ghana's cybersecurity challenges and reported that phishing and malware awareness was low among small businesses, making them vulnerable targets. These studies collectively suggest that although awareness of cyber threats is increasing, behavioral practices and reporting continue to lag across diverse socio-cultural settings.
- Whelan, C. et. al (2024) argued for a more contemporary and flexible framework. Using von Lampe's three primary domains of organized crime—criminal activities, offender social structures, and extra-legal governance—the paper emphasizes the relevance of violence and extra-legal governance in both physical and digital realms. It advocates for moving beyond debates about the existence of organized cybercrime to exploring new research questions by applying organized crime scholarship to cyber-criminal groups, proposing a reconceptualization of organized cybercrime.
- Indian Studies In India, research on cybercrime has expanded in the last decade alongside the growth of internet penetration.
- Gupta and Agarwal (2020) conducted a nationwide survey on cybersecurity awareness and reported that although respondents were familiar with common threats such as hacking, knowledge of ransomware and phishing was notably limited. Mishra, Sharma, and Yadav (2021) highlighted gender differences in perceptions of law enforcement in India, showing that women expressed greater hesitation in approaching authorities due to fear of harassment or reputational damage.
- Khan, S. et. al (2022) addressed the gap between rapidly advancing technology and the lagging cybercrime legislation. It emphasizes the critical role of legislation in combating cybercrime, highlighting the importance of

efficient and up-to-date legal responses. Using the "Preferred Reporting Items for Systematic Review and Meta-Analysis" method, the study systematically reviews literature across seven academic databases, ultimately analyzing 72 relevant studies out of 548 initial articles. The results emphasize the necessity of comprehensive and current cybercrime legislation to effectively counter cybercrime. The findings suggest that enhancing and updating legal frameworks is crucial to address the growing number of cybercrime incidents. The paper also identifies future research directions and practical implications for policymakers to strengthen legislative measures against cybercrime.

- A study by Singh and Kaur (2019) on college students in Punjab revealed that while more than 70% used strong passwords, less than half adopted two-factor authentication. NCRB (2022) data indicates that cyber fraud accounts for over 60% of registered cybercrime cases in India, yet underreporting remains significant. These findings underline the gap between theoretical awareness and actual safety practices, as well as the systemic barriers to effective reporting.

#### Theoretical Frameworks

The present study is guided by three key theoretical frameworks. First, Ajzen's Theory of Planned Behavior (1991) argues that behavioral intentions are shaped by attitudes, subjective norms, and perceived control. Applied to cybercrime, this theory suggests that awareness and confidence influence reporting readiness. Second, Bandura's Social Cognitive Theory (1986) emphasizes the role of observational learning, indicating that exposure to peers' practices can shape one's own digital safety habits. Third, Routine Activity Theory (Cohen & Felson, 1979) highlights the convergence of motivated offenders, suitable targets, and absence of capable guardians as drivers of victimization, which translates into the online environment through unsafe practices.

### 3. RESEARCH GAP

While existing literature highlights variations in awareness, practices, and reporting, there are still gaps in localized, data-driven studies in Rajasthan. Few studies have applied rigorous statistical methods such as chi-square tests, factor analysis, and regression to analyze cybercrime awareness and reporting behavior.

### 4. OBJECTIVES OF THE STUDY

The present study was undertaken with the following objectives:

1. To assess awareness of different types of cybercrime among internet users in Rajasthan.
2. To examine the extent to which respondents adopt safe online practices such as strong passwords, two-factor authentication, and system updates.
3. To evaluate knowledge and behavior related to reporting of cybercrime incidents.
4. To analyze demographic differences (gender and education level) in cybercrime awareness, safe practices, and reporting readiness.
5. To identify key predictors of cybercrime reporting readiness using regression analysis.

### Hypotheses of the Study

Based on the objectives and previous literature, the following hypotheses were formulated for statistical testing:

H1: There is no significant difference between male and female respondents in terms of cybercrime awareness.

H2: There is no significant difference between male and female respondents in safe online practices (cyber hygiene).

H3: There is no significant difference between respondents of different education levels (graduates and postgraduates) in cybercrime awareness and practices.

H4: Awareness, cyber threat literacy, and cybercrime response behavior do not significantly predict reporting readiness.

H5: There is no significant association between demographic factors (gender, education) and knowledge of reporting cybercrime.

These hypotheses were tested using chi-square tests, independent samples t-tests, and multiple regression analysis.

### 5. RESEARCH METHODOLOGY

#### Research Design

The study employed a descriptive and analytical research design based on a survey method. Primary data were collected through a structured questionnaire to measure awareness, practices, and reporting behavior related to cybercrime. The

design allowed for both descriptive analysis of respondent characteristics and inferential analysis using statistical tests to identify significant patterns.

### Sampling and Respondents

The study was conducted among internet users in Rajasthan. A sample size of 392 respondents was selected through stratified random sampling to ensure representation across gender and education levels. Out of the total respondents, 171 were male (43.6%) and 221 were female (56.4%). The majority were graduates (55%), followed by postgraduates (35%), with the remaining 10% from other educational categories. All respondents reported daily use of the internet and familiarity with the concept of cybercrime.

### Data Collection Instrument

A structured questionnaire was developed, comprising both closed-ended and Likert-scale questions. The questionnaire was divided into four sections:

1. Demographic profile (gender, age, education).
2. Awareness of various types of cybercrimes (scams, hacking, phishing, identity theft, ransomware, etc.).
3. Online safety practices (password strength, two-factor authentication, antivirus use, safe browsing habits).
4. Reporting knowledge and readiness (awareness of reporting portals, willingness to report, perceived barriers).

The instrument was pilot tested with 30 respondents to ensure clarity and reliability. Necessary modifications were made before administering the final survey.

### Reliability and Validity

Reliability of the instrument was measured using Cronbach's alpha, which yielded a value of 0.81, indicating good internal consistency. Content validity was ensured through expert consultation with academicians and cybercrime professionals. Construct validity was tested using exploratory factor analysis (EFA), which confirmed the presence of two dimensions: Cyber Literacy and Cyber Threat Literacy.

### Statistical Tools Used

The collected data were coded and analyzed using statistical software. The following tools were applied:

- Descriptive statistics: Frequencies, percentages, and mean scores for awareness and practices.
- Chi-square test: To test the association between demographic factors and awareness/practices.
- Factor analysis (PCA): To identify underlying dimensions of awareness and practices.
- Independent samples t-test: To compare mean scores across gender and education levels.
- Regression analysis: To determine predictors of reporting readiness.

The methodology ensured that both descriptive and inferential insights could be derived, supporting the research objectives and hypotheses.

## 6. DATA ANALYSIS AND RESULTS

The present section provides both descriptive and inferential statistical analysis of the primary survey conducted among 392 respondents in Rajasthan. Data are presented in the form of tables, charts, and test results, followed by interpretation.

### 6.1 DEMOGRAPHIC PROFILE OF RESPONDENTS

**Table -1:** Demographic Profile

Variable	Category	Frequency	percentage
Gender	Male	171	43.6%
	Female	221	56.4
Education	Graduate	216	55.0%
	Postgraduate	137	35.0%
	Others	39	10.0%

Interpretation: The sample was fairly balanced across gender, with a slightly higher representation of females. Education levels showed a dominance of graduates and postgraduates, ensuring that respondents had basic digital familiarity.

## 6.2 AWARENESS OF CYBERCRIMES

**Table -2:** Awareness of Different Types of Cybercrimes

Types of Cybercrime	Frequency	Awareness
Online scams & frauds	219	55.9%
Hacking	204	52.0%
Cyberbullying	112	28.6%
Honeytrap	82	20.9%
Phishing emails	78	19.9%
Identity theft	56	14.3%
Ransomware	36	9.2%

**Interpretation:** While general awareness of scams and hacking was high (above 50%), advanced threats such as phishing, identity theft, and ransomware had relatively low recognition, indicating knowledge gaps in digital literacy.

## 6.3 ADOPTION OF SAFE ONLINE PRACTICES

**Table -3:** Adoption of Safe Practices

Practice	Adoption (%)
Use of strong passwords	82.6
Different passwords	75.6
Two-factor authentication	66.3
Avoid suspicious links	82.2
Regular system updates	55.4

**Interpretation:** Most respondents adopted strong passwords and avoided suspicious links. However, fewer respondents regularly updated antivirus software or enabled two-factor authentication, leaving them vulnerable to cyber threats.

## 6.4 REPORTING KNOWLEDGE

**Table -4:** Knowledge of Reporting Cybercrime

Category	Percentage
Know how to report	42.9
Don't know	57.1

**Interpretation:** Less than half of the respondents knew how to report cybercrime. Barriers included lack of knowledge about portals, fear of lengthy legal procedures, and social stigma, highlighting a significant gap between awareness and reporting.

## 6.5 CHI-SQUARE TEST RESULTS

**Table -5:** Chi-square Test Results

Variable Tested	$\chi^2$ value	p-value	Result
Gender × Awareness of phishing	6.21	0.013	Significant
Gender × Awareness of scams	2.15	0.142	Not significant
Education × Safe practices	5.78	0.017	Significant

**Interpretation:** The chi-square test revealed significant associations between gender and awareness of phishing, as well as education and adoption of safe practices (e.g., 2FA). No significant gender difference was found for basic scams.

### 6.6 FACTOR ANALYSIS

Factor analysis using Principal Component Analysis (PCA) was applied to awareness and practices variables.

**Table -6:** Rotated Component Matrix

Variable	Factor 1 (Cyber Literacy)	Factor 2 (Cyber Threat Literacy)
Awareness of scams	0.782	—
Awareness of hacking	0.755	—
Awareness of phishing	—	0.701
Awareness of ransomware	—	0.689
Use of strong passwords	0.674	—
Two-factor authentication	0.648	—

KMO = 0.78, Bartlett’s Test =  $\chi^2 (45) = 542.16, p < 0.001$

**Interpretation:** Two key dimensions emerged – **Cyber Literacy** (basic awareness and safe practices) and **Cyber Threat Literacy** (advanced awareness). The test results confirmed sampling adequacy and factor reliability.

### 6.7 Independent Samples t-test

**Table -7:** Independent Samples t-test Results

Variable	Group	Mean	t-value	p-value	Result
Cyber hygiene	Male	3.89	2.31	0.021	Significant
	Female	3.62			
Reporting readiness	Male	3.25	2.12	0.035	Significant
	Female	3.47			
Threat literacy(education)	Graduate	3.41	1.76	0.081	Not significant
	Postgrad	3.56			

**Interpretation:** Males scored higher in cyber hygiene, while females showed greater readiness to report. Education level differences in threat literacy were present but not always significant.

### 6.8 Regression Analysis

**Table -8:** Regression Analysis Results  
**Dependent Variable:** Reporting Readiness

Predictor Variable	B	Beta	Sig.
Cybercrime Response	0.487	0.523	0.000
Awareness	0.212	0.271	0.002
Threat Literacy	0.156	0.196	0.010

Model Summary:  $R^2 = 0.462, F = 21.45, p < 0.001$

**Interpretation:** Cybercrime response behavior emerged as the strongest predictor of reporting readiness, followed by awareness and threat literacy. The model explained 46.2% of the variance in reporting readiness.

## Discussion

The findings of this study provide important insights into the patterns of cybercrime awareness, safe practices, and reporting behavior among internet users in Rajasthan. By combining descriptive and inferential statistics, the analysis not only describes the existing situation but also tests hypotheses about demographic differences and predictors of reporting readiness.

### Awareness and Knowledge Gaps

Results reveal that while general awareness of cybercrime is widespread, specific knowledge about advanced threats such as phishing (19.9%), identity theft (14.3%), and ransomware (9.2%) remains limited. This aligns with the findings of Gupta and Agarwal (2020), who reported similar gaps in Indian populations. Internationally, Lee (2015) and Yeboah-Boateng and Amanor (2014) also observed limited understanding of phishing and malware among students and small business owners. From a theoretical perspective, Bandura's Social Cognitive Theory (1986) suggests that without sufficient exposure or role models demonstrating safe online behavior, individuals may fail to develop advanced threat literacy.

### Safe Practices

Adoption of basic safety measures such as strong passwords (82.6%) and avoiding suspicious links (82.2%) was high, indicating that respondents are aware of common protective behaviors. However, adoption of two-factor authentication (66.3%) and regular system updates (55.4%) was relatively weaker. Singh and Kaur (2019) reported similar patterns among students in Punjab, highlighting a consistent gap between basic literacy and advanced practices. Routine Activity Theory (Cohen & Felson, 1979) provides an explanation: unsafe practices such as failing to update software increase the "suitability of targets," thereby raising the risk of victimization.

### Reporting Behavior

A significant gap was found in reporting knowledge, as only 42.9% of respondents knew how to report cybercrime. This reflects broader trends observed in NCRB (2022) data, where underreporting remains a major concern. Mishra et al. (2021) highlighted that social stigma and lack of trust in law enforcement are key barriers to reporting in India, especially for women. Interestingly, the present study found that women displayed slightly higher reporting readiness than men, despite men having higher technical literacy. This suggests that awareness campaigns should be designed to address both legal knowledge and psychological barriers.

### Gender and Education Differences

The t-test results indicated that males performed better in cyber hygiene and threat literacy, whereas females scored higher on reporting readiness. These findings partially support Mishra et al. (2021), who argued that gender differences are shaped by social expectations and trust in law enforcement. Education level differences showed that postgraduates had better awareness of advanced threats, consistent with Livingstone and Helsper (2007), who emphasized that higher education improves digital inclusion. However, the differences were not always statistically significant, suggesting that awareness campaigns should target all education levels rather than only focusing on advanced learners.

### Regression and Predictors of Reporting

The regression analysis confirmed that cybercrime response behavior is the strongest predictor of reporting readiness, followed by general awareness and threat literacy. This supports Ajzen's Theory of Planned Behavior (1991), which argues that behavior is influenced not just by knowledge but also by attitudes and perceived control. Individuals who had previously encountered cyber threats or practiced preventive measures were more confident in reporting. This highlights the importance of practical training and simulated exercises in awareness campaigns.

### Policy Significance

The study provides strong statistical evidence that while awareness exists, knowledge gaps, weak practices, and poor reporting knowledge undermine cyber safety. These findings have important policy implications for Rajasthan and India as a whole. Specifically, campaigns should emphasize advanced threats such as phishing and ransomware, promote technical safeguards like two-factor authentication, and simplify the reporting process to make it user-friendly. Schools, colleges, and community centers should be engaged to deliver targeted digital literacy programs.

## CONCLUSION AND POLICY IMPLICATIONS

The study set out to examine awareness, practices, and reporting behavior related to cybercrime among internet users in Rajasthan using primary data from 392 respondents. The statistical analysis revealed three key insights. First, while general awareness of cybercrime is universal, specific knowledge of advanced threats such as phishing, identity theft, and ransomware remains limited. Second, respondents widely adopted basic safe practices, such as using strong passwords and avoiding suspicious links, but adoption of technical safeguards like two-factor authentication and regular updates was relatively weak. Third, although nearly all respondents were aware of cybercrime in principle, fewer than half knew how to report incidents, highlighting a critical gap between knowledge and legal action.

Gender and education-level comparisons further enriched the findings. Men demonstrated stronger cyber hygiene and threat literacy, whereas women expressed slightly greater readiness to report incidents. Postgraduates had somewhat better knowledge of advanced threats, but differences were not always statistically significant. Regression analysis confirmed that cybercrime response behavior is the strongest predictor of reporting readiness, followed by awareness and threat literacy.

Based on these findings, the following **policy implications** are suggested:

1. **Targeted Awareness Campaigns:** Public campaigns should emphasize less-known threats such as phishing, identity theft, and ransomware, alongside basic awareness.
2. **Strengthening Safe Practices:** Programs should encourage widespread adoption of two-factor authentication, frequent system updates, and antivirus use.
3. **Gender-Sensitive Digital Literacy:** Special initiatives should be designed for women to strengthen both cyber hygiene and confidence in reporting.
4. **Simplified Reporting Mechanisms:** Reporting procedures should be made more user-friendly through online portals, mobile apps, and awareness drives about the National Cyber Crime Reporting Portal.
5. **Integration into Education:** Cyber literacy modules should be incorporated into school and college curricula to ensure early exposure and consistent practices.

In conclusion, this research contributes to the academic understanding of cybercrime behavior through statistical analysis while offering actionable recommendations for policymakers, educators, and law enforcement. By bridging the gap between awareness, practice, and reporting, Rajasthan can build a stronger culture of digital safety and resilience.

## Limitations and Future Scope

Like all empirical research, this study has certain limitations. First, the survey was conducted only in Rajasthan, which may limit the generalizability of the findings to other states of India with different socio-economic and cultural conditions. Second, the sample primarily comprised educated respondents (graduates and postgraduates), which means that the perspectives of less-educated or rural populations may be underrepresented. Third, the reliance on self-reported data introduces the possibility of response bias, as participants may overstate their safe practices or underreport their vulnerabilities.

Future research can address these limitations by adopting a multi-state comparative design that includes both urban and rural populations. Expanding the sample to cover different age groups and occupations will provide a more comprehensive picture of cybercrime awareness and practices. In addition, longitudinal studies could be conducted to track changes in awareness and reporting behavior over time. Finally, qualitative methods such as interviews or focus groups can be used to explore in greater depth the psychological and social barriers to reporting cybercrime.

## REFERENCES

- [1]. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
- [2]. Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- [3]. Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- [4]. Gupta, R., & Agarwal, S. (2020). Cybersecurity awareness in India: A survey-based analysis. *International Journal of Cyber Studies*, 5(1), 45–62.

- [5]. Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1–25.
- [6]. Horan, C., & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, 1(4), 580-596
- [7]. Lee, S. (2015). Cyberbullying and youth: Risk factors and prevention strategies. *Asian Journal of Communication*, 25(1), 59–77.
- [8]. Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: Children, young people, and the digital divide. *New Media & Society*, 9(4), 671–696.
- [9]. Mishra, P., Sharma, R., & Yadav, N. (2021). Gender differences in trust toward law enforcement in India. *Journal of Social Policy Research*, 12(3), 210–225.
- [10]. National Crime Records Bureau (NCRB). (2023). *Crime in India 2023: Statistics*. Government of India, Ministry of Home Affairs.
- [11]. Singh, K., & Kaur, M. (2019). Cyber hygiene practices among students: A case study of Punjab. *Journal of Information Security Research*, 8(2), 55–67.
- [12]. Whelan, C., Bright, D., & Martin, J. (2024). Reconceptualising organised (cyber) crime: The case of ransomware. *Journal of Criminology*, 57(1), 45-61.
- [13]. Williams, M. L. (2006). *Virtually criminal: Crime, deviance and regulation online*. Routledge.
- [14]. Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297–307.

## BIOGRAPHIES



Deepak kumar Parewa earned a B,Sc And M.Sc MSC from University of Rajasthan Jaipur in 2017 and 2019. Currently pursuing a Ph.D. with a specialization in Statistics, Department of Statistics from University of Rajasthan, Jaipur. He is a member of IJJET since 2025. He has published more than two research paper in reputed international journals and conferences



Dr Deepa Mordia earned a B.Sc., M.Sc. and Ph.D. from University of Rajasthan, Jaipur in 2001, 2003 and 2018. She is a currently working as Assistant professor in Department of Statics since from University of Rajasthan Jaipur since 2018. She has 18 years of teaching experience and 12 years of research experience. The earlier job involved teaching the Under Graduate and Post Graduate student of the Management branch (MBA, BBA), Computer Science, Electronics Mechanical, Civil, Computer Application and Post Graduate student of Bio-informatics and M.Tech She has published more than 50 resources paper in reputed International General and Conference.