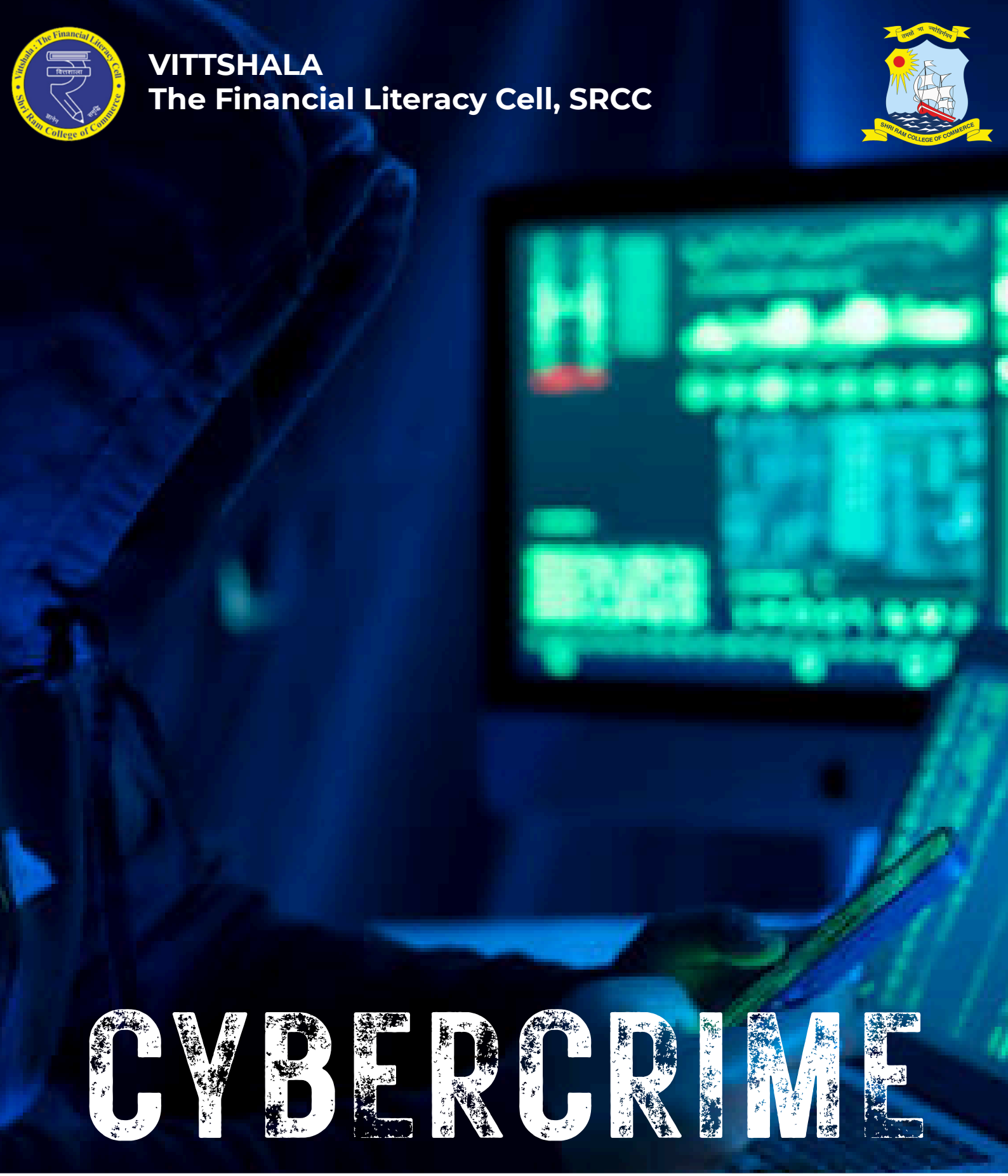
VITTSHALA
The Financial Literacy Cell, SRCC



CYBERCRIME

Research Report 2025-2026

TABLE OF CONTENTS

1 INTRODUCTION 1

2 LITERATURE REVIEW 2

3 METHODOLOGY 4

4 ANALYSIS AND INTERPRETATION 6

5 STATISTICAL ANALYSIS 10

6 CONCLUSION 20

7 APPENDIX 21

Introduction

The rapid growth of internet usage and digital technologies has significantly transformed the social and economic landscape of India. With increased access to smartphones, affordable data services, and the widespread adoption of digital payment systems, individuals are more connected than ever before. However, this digital expansion has also led to a sharp rise in cybercrime, making it a major concern for individuals, businesses, and policymakers. Cybercrime includes a wide range of illegal activities such as phishing, identity theft, online financial fraud, hacking, ransomware attacks, and misinformation through emerging tools like deepfakes.

In recent years, initiatives such as Digital India have accelerated online engagement, but awareness and preparedness among users have not always kept pace with the evolving nature of cyber threats. Many users continue to lack adequate knowledge about cyber risks, safe online practices, and legal protections such as those provided under the Information Technology Act, 2000. This gap between digital adoption and cybersecurity awareness increases vulnerability, particularly among certain demographic groups.

This research paper aims to examine the awareness, perception, and experiences related to cybercrime among internet users in India. The study is based on primary data collected from over 300 respondents across different age groups, genders, educational backgrounds, and occupations. A structured questionnaire was used to assess familiarity with various cyber threats, digital payment usage, personal experiences with cybercrime, and attitudes towards cybersecurity measures and law enforcement.

To ensure a comprehensive analysis, various statistical techniques such as correlation, analysis of variance (ANOVA), regression, and chi-square tests have been applied. These methods help identify relationships between demographic factors, awareness levels, behavioral patterns, and vulnerability to cybercrime. The findings of this study aim to provide insights into current awareness levels and suggest measures to strengthen cybersecurity practices and policies in India.

Literature Review

The rapid expansion of digital infrastructure in India over the past decade has brought with it a sharp rise in cybercrime, making it one of the most serious concerns for policymakers, law enforcement, and ordinary internet users alike. While scholarly work across disciplines has begun to map the intricacies of this problem, significant gaps remain, particularly in understanding how awareness, behavior, and legal response intersect at the ground level.

Research published in academic journals on information security has consistently noted that India's growing internet user base, while a marker of digital progress, has also simultaneously expanded the attack surface for cybercriminals. Studies highlight phishing, financial fraud, identity theft, and hacking as the most prevalent forms of cybercrime affecting Indian users. Something striking across this body of work is the finding that a majority of victims had little to no prior awareness of the threats they encountered. Users frequently engaged in high-risk behaviors, reusing passwords, clicking on unverified links, and sharing sensitive information over unsecured platforms, not out of carelessness but out of a genuine lack of cybersecurity literacy. This suggests that the problem is not merely technical but deeply educational.

The legal dimension of cybercrime in India has also attracted scholarly attention. Research examining the country's regulatory framework points to the Information Technology Act of 2000 and its subsequent amendments as the primary legislative response to digital offenses. While the Act covers a broad range of cybercrimes and prescribes penalties accordingly, scholars have raised questions about its practical effectiveness. Challenges such as underreporting of offenses, insufficient training of law enforcement personnel, slow judicial processes, and jurisdictional complications in cross-border cybercrime cases limit the law's reach. There appears to be a disconnect between what the legislation promises on paper and what citizens actually experience in terms of justice and redressal.

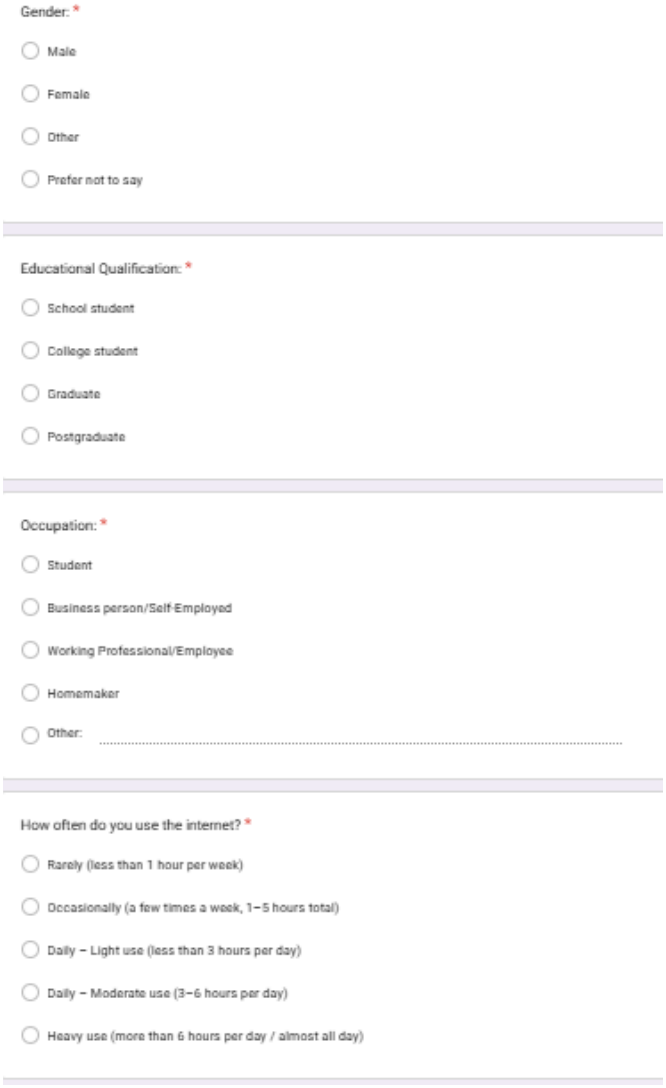
An important pattern emerging across these studies is the urban-centric focus of most research. The majority of existing surveys and analyses concentrate on metropolitan or semi-urban populations, leaving rural and semi-literate internet users who are increasingly coming online through mobile-first access largely underexamined. Additionally, most prior work relies on secondary data or small convenience samples, which limits the generalizability of findings.

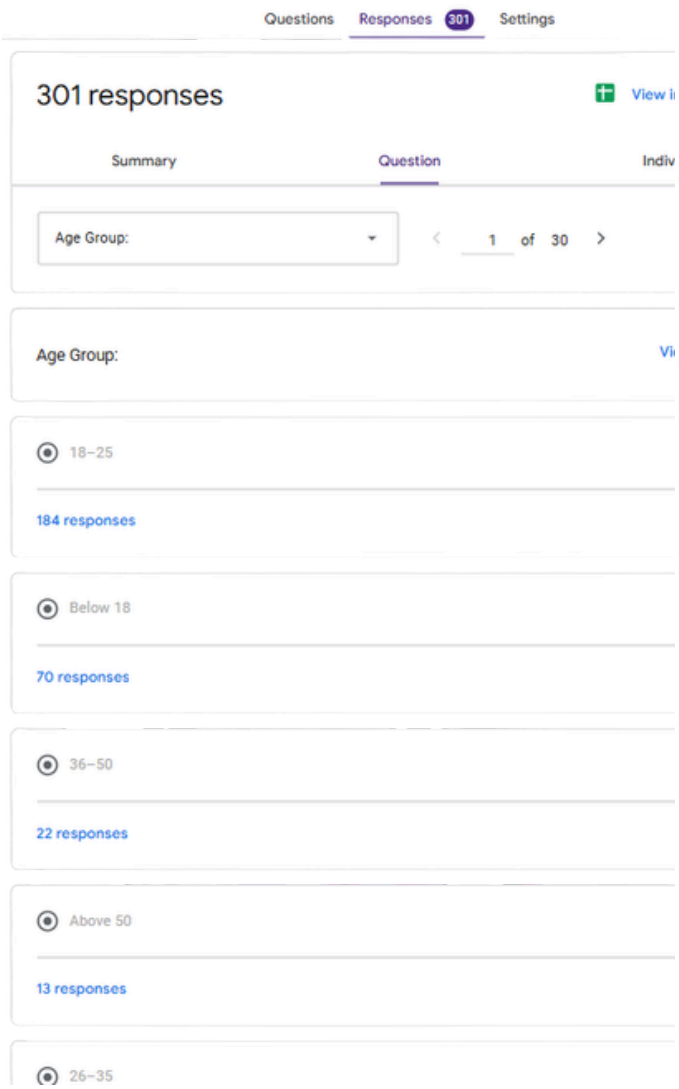
This is precisely the gap the present study aims to address. By collecting primary data directly from respondents and applying statistical analysis, this research seeks to offer a more grounded, representative picture of cybercrime awareness, victimization patterns, and perceived effectiveness of legal safeguards across a wider demographic. Where existing literature provides context and theoretical grounding, this study contributes empirical evidence that can inform more targeted interventions.

Methodology

This study adopts a descriptive and analytical research design using a quantitative approach to examine awareness, behavior, and perceptions related to cybercrime. The research is primarily based on primary data collected through a structured questionnaire designed to capture responses across multiple dimensions, including demographic characteristics, awareness levels, online behavior, and personal experiences with cybercrime.

The data was collected using an online survey method, with responses gathered from over 300 participants across diverse age groups, educational backgrounds, and occupations. A convenience sampling technique was used, as respondents were selected based on accessibility and willingness to participate. The questionnaire included a mix of multiple-choice questions, Likert scale-based items, and a few open-ended responses to ensure both quantitative depth and contextual understanding.





A key component of the study is the Awareness Score, which was constructed to measure respondents' familiarity with various cyber threats. This score was calculated by taking the average of responses to multiple items assessing familiarity with threats such as phishing, identity theft, ransomware, deepfakes, online financial fraud, and malware.

For data analysis, several statistical techniques were employed to derive meaningful insights. Correlation analysis was used to examine relationships between awareness levels and online behavior, while ANOVA was applied to identify differences in awareness across demographic groups. Regression analysis helped assess the impact of variables such as education and internet usage on awareness levels, and the chi-square test was used to analyze associations between categorical variables such as victimization and behavioral patterns.

The data was processed and analyzed using spreadsheet-based tools, ensuring systematic organization and interpretation. While the study provides valuable insights, it is subject to limitations such as reliance on self-reported data and the use of non-probability sampling, which may affect the generalizability of the findings.

Despite providing valuable insights, the study is subject to certain limitations. The use of a convenience sampling technique may limit the generalizability of the findings, as the sample may not fully represent the broader population. Additionally, the data is based on self-reported responses, which may be affected by response bias, social desirability bias, or inaccurate recall. The study also relies on an online survey method, which may exclude individuals with limited internet access or lower digital literacy, thereby potentially skewing the results. Furthermore, while statistical techniques have been applied to analyze relationships and patterns, the cross-sectional nature of the data restricts the ability to establish causal relationships between variables.

Analysis and Interpretation

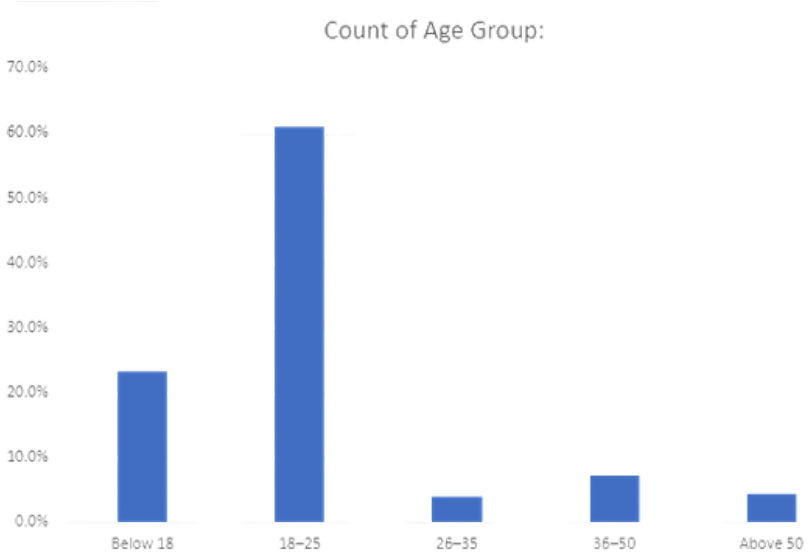


Figure 1: Age Group distribution chart

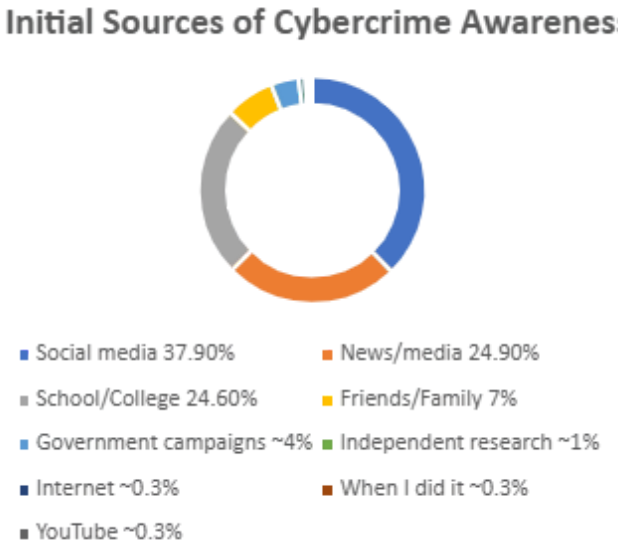
The adjacent diagram illustrates the distribution of respondents across various age categories to identify the primary demographic of internet users in this study.

Key Insight: A significant majority, over 60% of respondents, fall within the 18-25 age group, indicating that the findings primarily reflect the digital experiences and awareness levels of Gen Z and young university students.

Figure 2: Initial Sources of Cybercrime Awareness

The adjacent diagram illustrates the various primary channels through which respondents first encountered information regarding cybercrime to evaluate the effectiveness of different awareness platforms.

Key Insight: Social media serves as the most dominant information channel, accounting for 37.90% of initial awareness, while traditional Government campaigns lag significantly at approximately 4%.



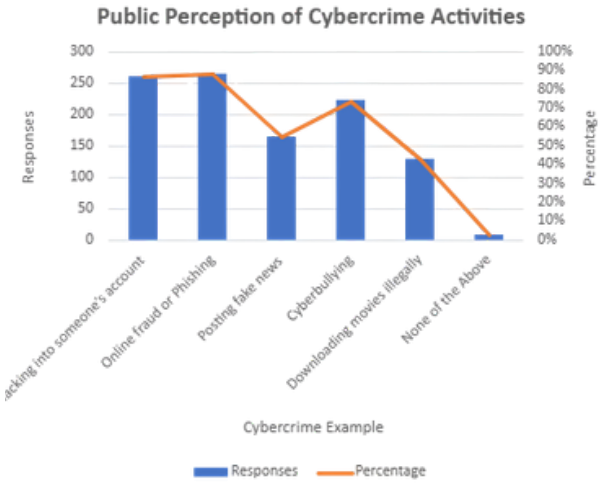


Figure 3: Public Perception of Cybercrime Activities

The adjacent diagram illustrates the extent to which respondents identify various online activities as criminal offenses to assess the general public's understanding of the legal boundaries of the digital landscape.

Key Insight: While traditional crimes like Hacking and Online Fraud are recognized by over 85% of the population, a notable awareness gap exists for "Downloading movies illegally," which is identified as a cybercrime by only about 40% of respondents.

Figure 4: Legal Literacy & Reporting Awareness

The adjacent diagram illustrates the extent of public knowledge regarding India's cybercrime laws (such as the IT Act, 2000) and official reporting channels like the 1930 Helpline and national portals.

Key Insight: A significant knowledge gap exists in the redressal landscape, as less than 10% of respondents are aware of both the legal framework and the correct reporting channels, while the majority have either only heard of them or remain completely unaware.

Figure 5: Comparative Analysis of Cyber Threat Familiarity

The adjacent diagram illustrates the varying levels of respondent familiarity across different categories of cyber threats, measured on a scale from 1 (Not Familiar) to 5 (Very Familiar), to identify specific technical knowledge gaps in the digital landscape.

Key Insight: While online scams show the highest familiarity, with over 130 respondents ranking themselves as "Very Familiar" (Score 5), advanced threats like ransomware show a critical awareness deficit, with the highest concentration of users (nearly 100) reporting they are "Not Familiar" at all.

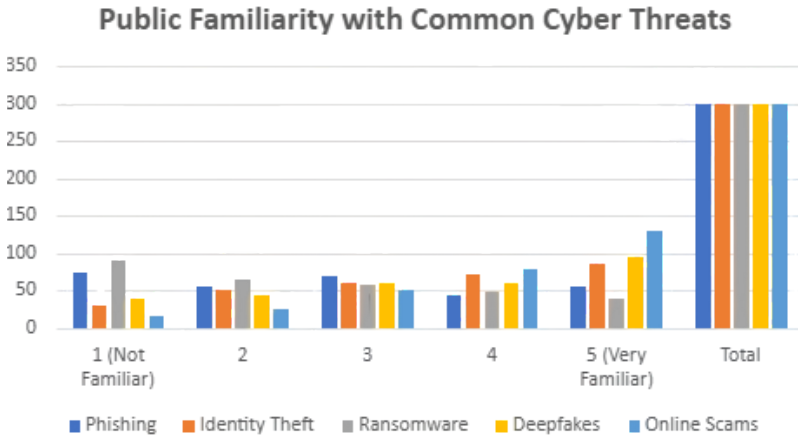
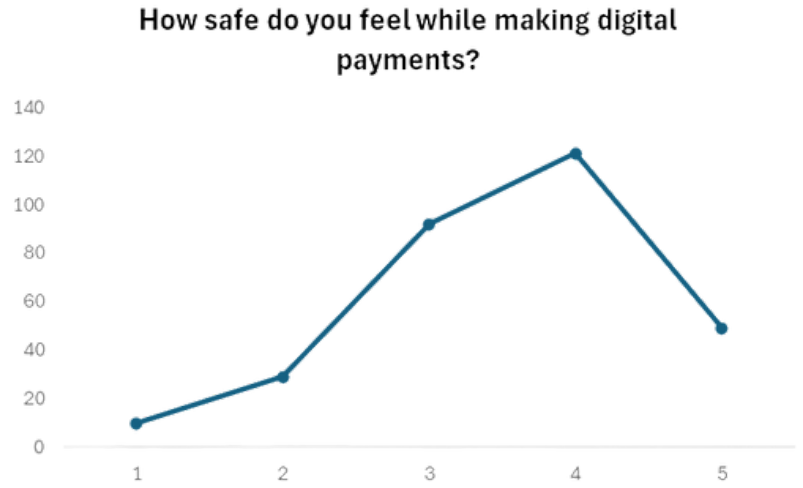


Figure 6: Perceived Safety in Digital Payments

The adjacent diagram illustrates the levels of safety respondents feel while making digital payments, measured on a scale from 1 (Very Unsafe) to 5 (Very Safe), to gauge public trust in digital financial systems.

Key Insight: While the majority of users express a relatively high level of trust, with a peak of over 120 respondents rating their safety at a 4/5, there remains a cautious sentiment as fewer than 50 users feel "Very Safe" (5/5) despite the widespread adoption of digital payment methods.



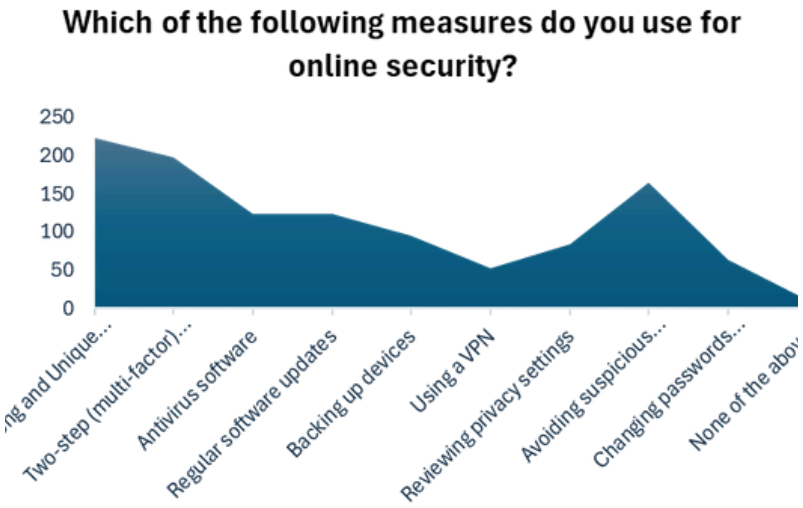


Figure 7: Adoption of Online Security Measures

The adjacent diagram illustrates the specific proactive measures respondents utilize to secure their digital identities and data, highlighting the most and least common protective behaviors in the sample.

Key Insight: While foundational habits like using strong and unique passwords and two-step (multi-factor) authentication are highly adopted by over 200 respondents, more advanced tools like VPNs remain underutilized, suggesting a preference for basic settings over comprehensive technical protection.

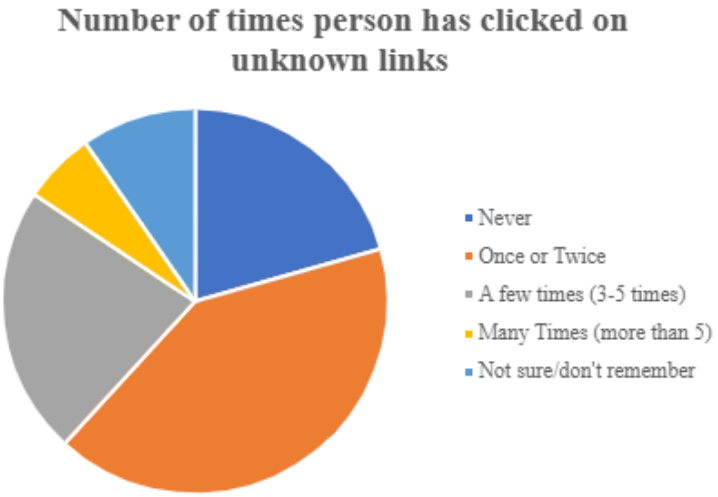


Figure 8: Frequency of Interaction with Unknown Links

The adjacent diagram illustrates the frequency with which respondents have clicked on unknown links or attachments, serving as a critical indicator of behavioral vulnerability to phishing and malware-based cyberattacks.

Key Insight: A significant majority of respondents, approximately 80%, admit to having clicked on unknown links at least once, with over 40% doing so "Once or Twice," highlighting that human curiosity remains the most common entry point for digital security breaches.

Figure 9: Perceived Susceptibility of Online Activities

The adjacent diagram illustrates which digital activities respondents believe are most vulnerable to cyberattacks, helping to identify where users feel the greatest sense of risk in their daily online interactions.

Key Insight: Online Banking is overwhelmingly perceived as the most susceptible activity, with 100 respondents identifying it as a primary target, followed closely by downloading files, while Online Gaming is seen as the least risky.

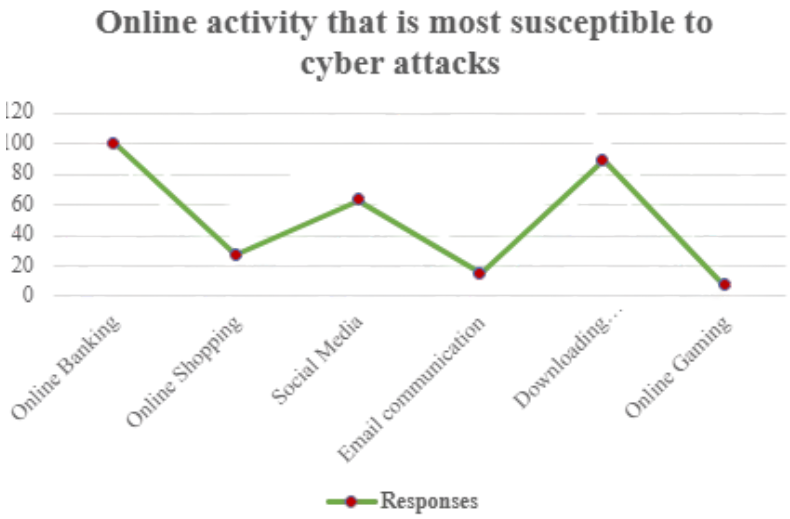


Figure 10: Crime Typology among Victims

The adjacent diagram illustrates the specific categories of cybercrime experienced by respondents or their immediate acquaintances, helping to identify the most prevalent threats in the current digital landscape.

Key Insight: Financial fraud or UPI scams emerged as the single most frequent threat, affecting 127 respondents, which is nearly double the rate of online shopping scams (66) or social media hacking (60), underscoring a critical need for enhanced security in digital financial transactions.

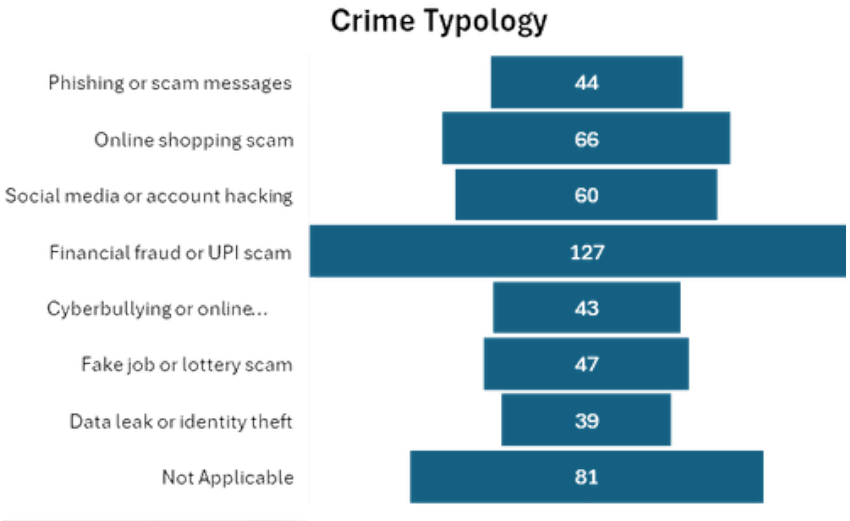


Figure 11: Incident Response & Outcome Analysis

The adjacent diagram illustrates the actions taken by victims following a cybercrime incident and the subsequent effectiveness of various redressal channels, highlighting the challenges in obtaining successful resolutions.

Key Insight: A critical gap in law enforcement efficacy is evident, as nearly 45% of those who approached authorities (39 out of 88 total reporters) felt they "got no help," while a combined 12% of victims chose not to report at all due to a lack of knowledge or perceived insignificance of the crime.

Figure 12: Public Demand for Academic Cyber Security Training

The adjacent diagram illustrates the level of public agreement regarding the inclusion of cyber safety as a compulsory part of school and college curricula, measured on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Key Insight: There is overwhelming institutional demand for academic reform, with nearly 75% of respondents giving a rating of 4 or 5, signifying a collective belief that formal education is the most critical long-term defense against the rising tide of cybercrime.

Statistical Analysis

CHI-SQUARE TEST

A chi-square test is a statistical test that analyses whether two groups (categorical values) are related or not. It looks at both groups' actual number of occurrences (observed frequencies) and the number of occurrences (expected). If the observed value is much larger or smaller than expected, that indicates a relationship between the two groups. If the two groups differ only slightly, that indicates that the observed difference could be a random occurrence.

This test fit the study perfectly since the survey yielded data that was mostly categorical, covering aspects like how aware people are, their behavior patterns, different demographic groups, and their victimization experiences. This analysis sought to explore connections between various factors, such as whether having more awareness impacts security behavior or if engaging in risky activities is associated with victimization. Given that the Chi-square test is tailored for exploring connections among categorical data and assessing the significance of observed differences, it was the best choice for our report.

Formula For Chi-Square Test:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

Symbols are broken down as follows:

- O_i: Observed frequency
- E_i: Expected frequency

Interpreting Results:

- If the p-value is less than a certain significance level (e.g., 0.05), then the null hypothesis is rejected, which is commonly denoted by α. Thus, it means that category variables highly correlate with each other.

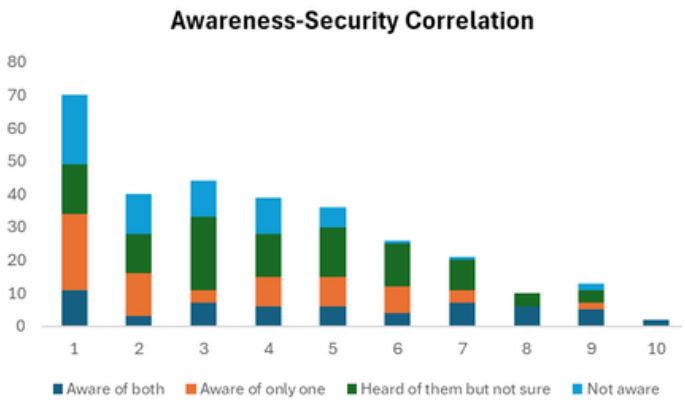
- When a p-value is above α, it implies that the null hypothesis cannot be rejected; hence, there is insufficient evidence for establishing the relationship between these variables.

1. Awareness vs Security Behaviour

The test was conducted to examine the relationship between awareness of cybercrime laws and the adoption of security measures. **The p-value obtained was 0.0013**, which is significantly lower than the conventional significance level of 0.05, indicating a very strong statistical association between the two variables.

Due to the very low p-value, it is unlikely that the differences in security behaviours across the different levels of awareness were simply due to chance. In essence, awareness is not just a theoretical concept but is converted into behaviour that can be measured in actual use. More specifically, survey respondents who were aware of laws and reporting mechanisms related to cybercrime are more likely to adopt a larger number of security measures than those who are unaware. Examples of this include the use of strong passwords, multi-factor authentication, and taking precautions while engaging in online activity.

This relationship highlights the effectiveness of awareness as a tool for behavioural change, suggesting that individuals who are informed about cyber risks and legal frameworks are more proactive in safeguarding themselves. It also implies that awareness initiatives, educational campaigns, and policy-level interventions can play a critical role in strengthening cybersecurity practices among users.



2. Response to Cybercrime vs Trust in Law Enforcement

While conducting the test, the **p-value obtained was 0.7918**, which is substantially higher than 0.05, indicating no statistically significant association between the variables.

The high p-value indicates that the trust levels of respondents across the different response categories (i.e., reporting, not reporting, dealing with it informally) are minimal and likely due to chance. That is, individuals' behaviours in regard to cybercrime incidents do not have a direct effect on their trust in law enforcement.

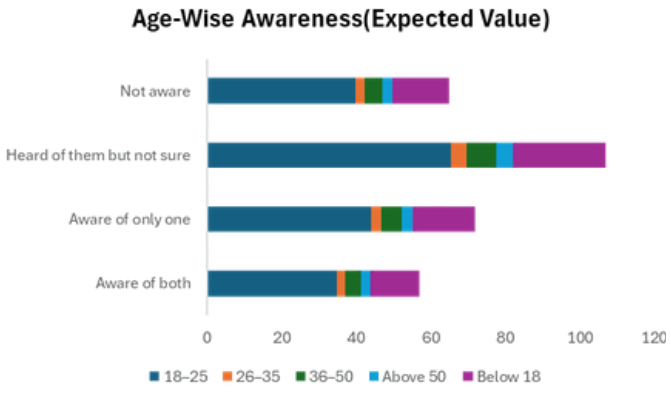
This could indicate a broader, more uniform perception of law enforcement that is not strongly shaped by personal response behaviour. It may also reflect limited direct interaction with authorities or a general lack of awareness about formal reporting mechanisms, leading to similar trust levels regardless of how individuals respond to cyber incidents.

3. Age vs Awareness of Laws

A chi-square test was conducted to examine the relationship between age group and how much people know about cybercrime legislation. **A p-value of 0.5264 was obtained,** which is much greater than the 0.05 significance level; therefore, there is not a statistically significant association between the age group and levels of awareness.

The relatively high p-value suggests levels of awareness of cybercrime laws are generally equal across age categories in our sample, with no evidence to suggest that any levels of awareness differ significantly. Therefore, it appears levels of awareness are not restricted to one age category and are distributed evenly across all age groups.

This type of pattern may be a function of the extensive use of technology, similar access to digital resources for acquiring cybercrime information, and large-scale general awareness campaigns targeting individuals residing in multiple age categories, thereby providing individuals with similar levels of knowledge despite their age.



4. Gender × Victimization

The p-value acquired was 0.8362, which is much higher than the significance level of 0.05; thus, between gender and likelihood of falling prey to cybercrime, no statistically significant relationship is observed.

A very high p-value means that there is hardly any difference in the distribution of victimization among genders. Any small differences seen in the data are probably due to random chance rather than a systematic effect. This means that the risk of becoming a victim of cybercrime does not differ on the basis of gender within the sample handled in this study and equally affects individuals.

5. Risky Behaviour × Victimization

A chi-square test was conducted to examine the relationship between risky online behaviour (such as clicking unknown links) and cybercrime victimization. **The p-value obtained was 0.3593**, which is greater than 0.05, indicating that the association between these variables is not statistically significant.

Although risky behaviour should theoretically make one more vulnerable, the p-value obtained indicates the differences in victimization between risk groups that do not lend themselves to a pattern reliable enough to apply across individuals.

However, a closer look at the data may still reveal that there are still detectable differences between people who engage more in risky behaviour and people who are victims of it. The lack of their statistical significance suggests that this trend is not definite and may be influenced by other components such as awareness, prevention factors, or events explained by chance.

CORRELATION TEST

A correlation test is a statistical technique that allows researchers to measure the relationship between two variables. In this case, the test applies the Pearson correlation coefficient (r). Its range of values goes from -1 to +1. If a value tends toward +1, it indicates a strong positive correlation between two variables; if it is closer to -1, it indicates a strong negative correlation. The closer the r is to zero, the less related the two variables are considered.

The correlation test will be appropriate in this research because some variables are quantitative or ordinal, meaning some data are continuous. These include awareness score, level of perceived safety, and behavioral parameters.

Degree of Correlation	Positive Correlation	Negative Correlation
Perfect Correlation	1	-1
Very High Degree of Correlation	0.9	-0.9
Fairly High Degree of Correlation	Between +0.75 and +0.9	Between -0.75 and -0.9
Moderate Degree of Correlation	Between +0.25 and +0.75	Between -0.25 and -0.75
Low Degree of Correlation	Between 0 and +0.25	Between 0 and -0.25
Zero/No Correlation (uncorrelated)	0	0

1. **Trust in Law Enforcement vs Willingness to Engage**

After performing the correlation analysis on trust in law enforcement and willingness to engage in cybersecurity, the **result was an r equal to 0.153**, which signifies a very weak positive correlation. Respondents with varying levels of trust showed different degrees of willingness, implying that participation depends on other parameters like personal interest, awareness, or convenience rather than institutional trust.

2. Awareness Score vs Perceived Safety in Digital Payments

The relationship between awareness scores and safety during digital payments was calculated as **r = 0.307,** implying a moderate positive relationship.

This means that people who are more aware of cyber threats generally feel safe when using digital payment services. The reason for that may be that people become more confident in their ability to use the Internet safely, and the relationship can also suggest that some other parameters contribute to their risk perception.

1	
0.307	1

3. Internet Exposure vs Risky Behaviour

The correlation between internet usage and risk-taking behavior, such as opening suspicious websites/emails, is low positive **(r = 0.086).**

This suggests that people do not become more likely to perform risky behavior just because they use the Internet frequently. In fact, regular users can accumulate knowledge of online threats and reduce the risks associated with their behavior.

4. Awareness Score vs Risky Behaviour

The correlation between awareness score and risky online behavior is **r = 0.011**. However, from the above observations, we can conclude that although people might have enough knowledge regarding cybercrimes, they may act based on their instincts or habits rather than the information provided during the awareness campaigns.

1	
0.011039068	1

5. Awareness Score vs Perceived Risk of Victimisation

The awareness scores had a correlation of **r = –0.096** with the perception about the likelihood of becoming a victim of cybercrime.

This implies that individuals who are more aware of cybersecurity issues will have a lower perception of becoming a target. The very low relationship shows that people's awareness is independent of their perception of becoming a victim of cybercrime, since the relationship is very weak.

Overall Analysis

From the analysis, it is clear that awareness has limited effect on most behavioral outcomes, though it does show a moderate positive relationship with confidence in digital payments. However, it has very minimal effects on the actual cybersecurity behavior of the respondents, and most correlations were very low.

In conclusion, we have established that although awareness has some impact on people's behavior, there are other variables influencing this behavior apart from awareness.

REGRESSION ANALYSIS

Regression analysis is a statistical technique used to examine the relationship between a dependent variable and one or more independent variables, enabling the measurement of how changes in certain factors influence an outcome. It is represented by the equation **Y = a + bX + e, where Y is the dependent variable, X represents the independent variable(s), 'a' is the constant, 'b' is the coefficient indicating the impact of X on Y, and 'e' is the error term.** In the present dataset, which is based on survey responses related to cybercrime awareness, victimization, and reporting behaviour, regression analysis is highly suitable as it allows for a systematic and quantitative evaluation of relationships among multiple variables such as age, gender, education, awareness, and digital usage. It not only helps in identifying significant predictors but also provides statistical evidence through indicators like coefficients, R^2 values, p-values, and F-tests, making the analysis reliable and meaningful.

Multiple Regression:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n + \epsilon$$

Where

- Y is the predicted output,
- X1,X2,…,Xn are independent input variables,
- β0is the intercept term,
- β1,β2,…,βn are weight of each feature,
- n is number of input variables,
- ϵ is the error term.

1. Predicting awareness level

Awareness was taken as the dependent variable, while demographic factors such as age, gender, and education level were considered independent variables. The obtained results indicate that education level has a positive and statistically significant impact on awareness, suggesting that individuals with higher educational qualifications tend to have greater knowledge about cybercrime. The coefficient for education is positive, showing a direct relationship, while its p-value is below the acceptable significance level, confirming the reliability of this effect. On the other hand, variables such as gender and age show comparatively weaker or statistically insignificant relationships, indicating that their influence on awareness is limited. The R^2 value suggests that a moderate proportion of variation in awareness is explained by these variables, meaning that while the model is useful, other external factors may also play a role in determining awareness levels.

Metric	Value	Interpretation
R-Squared	**0.060646655**	Weak Explanatory Power: The model explains roughly 6% of the variance. While significant, the effect size is small.
Adjusted R-Squared	**0.051158237**	Adjusted Fit: After penalizing for the number of predictors, the model accounts for 5.1% of the data's variance.
Significance F	**0.000328768**	Highly Significant: The p-value is well below 0.05, meaning there is a less than 0.1% chance the results are due to random noise.

2. Predicting victimization

Victimization was considered the dependent variable, with awareness, demographic factors, and digital behaviour as independent variables. The obtained results show that the overall model is not statistically significant, as indicated by a Significance F value of 0.166, which exceeds the standard 0.05 threshold. This suggests that the combination of awareness, demographics, and digital behaviour does not reliably predict victimization in this dataset. The R^2 value of 0.026 indicates that only approximately 2.6% of the variation in victimization is explained by the included variables, leaving over 97% of the variance unaccounted for. Furthermore, because the overall model fails the significance test, any observed relationships, such as the potential negative relationship between awareness and victimization, cannot be confidently generalized. This implies that victimization is likely driven by multiple external, situational, or technical factors.

Metric	Value
R-Squared	**0.026030808**
Adjusted R-Squared	**0.009522855**
Significance F	**0.166426976**

3. Predicting reporting of cybercrimes

Reporting behaviour was taken as the dependent variable, while factors such as awareness level, prior victimization, and demographic characteristics were used as independent variables. The obtained results show that the model is not statistically significant, as evidenced by a Significance F value of 0.93, which is well above the standard threshold of 0.05. This implies that awareness, prior victimization, and demographic characteristics do not have a reliable or predictable impact on reporting behaviour within this data set.

The R^2 value of 0.008 indicates a negligible explanatory power, showing that these variables explain less than 1% of the variation in reporting behaviour. Furthermore, the negative Adjusted R-Squared confirms that the model is a very poor fit for the data. Consequently, the results suggest that reporting behaviour is not driven by the factors tested here, and that other unobserved variables, such as trust in authorities, the complexity of reporting processes, or cultural factors, likely play a much more dominant role.

Metric	Value	Interpretation
R-Squared	**0.008254837**	Negligible Fit: Less than 1% of reporting behavior is explained by this model.
Adjusted R-Squared	**-0.01543873**	Weak Model: The negative value indicates the model is a very poor fit for the data..
Significance F	**0.930861703**	Not Significant: The model fails to show any reliable relationship between the variables (p > 0.05).

Conclusion:

Overall, the regression results across all three analyses highlight important patterns in the dataset. Awareness emerges as a key variable, both as a dependent factor influenced by education and as an independent factor reducing victimization and encouraging reporting behaviour. The significance levels indicate that not all variables contribute equally, and only a few key predictors play a meaningful role. The R^2 values across models suggest moderate explanatory power, indicating that while regression provides valuable insights, there are additional external influences that are not captured in the analysis. In conclusion, regression analysis proves to be an effective method for understanding the relationships between awareness, victimization, and reporting of cybercrimes, offering meaningful insights that can help in designing better awareness programs, preventive strategies, and reporting mechanisms.

ANOVA

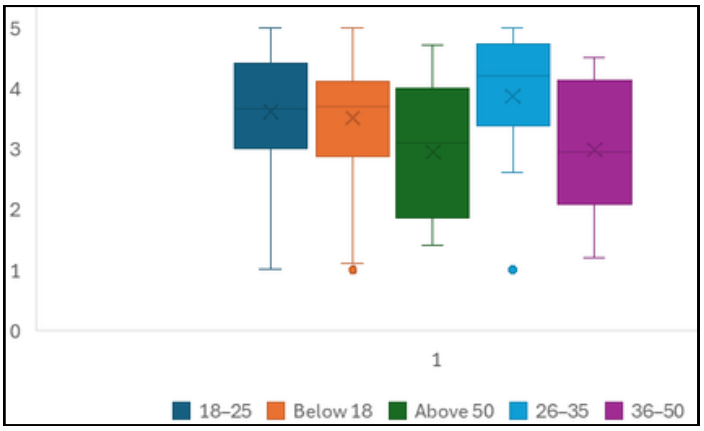
ANOVA (Analysis of Variance) is a statistical technique used to examine whether there are significant differences between the means of multiple groups by comparing variation between groups and within groups. It relies on the F-value and p-value to determine significance, where a p-value less than 0.05 indicates a statistically significant relationship, and a value greater than 0.05 indicates no significant difference. This method is suitable for the dataset as it involves comparing different categorical independent variables (such as age, behavior, education, and experience) with dependent variables like awareness, protection, trust, and security practices.

Assumptions of ANOVA:

1. **Independence:** Observations are randomly sampled, and groups are independent.
2. **Normality:** Residuals (errors) are approximately normally distributed.
3. **Homoscedasticity:** Equal variances across groups.

1. Age group and overall familiarity:

The ANOVA results show a **p-value of approximately 0.0618**, which is slightly higher than the significance level of 0.05. This indicates that there is no statistically significant difference in familiarity levels across different age groups. However, since the value is close to 0.05, it suggests a weak trend where age may have some minor influence on familiarity, but not strong enough to be considered statistically significant.



2. Risky behavior and protection

The ANOVA results show a p-value of **0.00547**, which is significantly lower than 0.05. This clearly indicates a statistically significant relationship between risky behavior and protection levels. It implies that individuals engaging in different levels of risky online behavior show meaningful differences in how they adopt protective measures, making risky behavior a key influencing factor in cybersecurity practices.

3. Victim experience and police trust

The p-value is approximately **0.0596**, which is slightly above 0.05. This suggests that there is no statistically significant difference in trust in police across different levels of victim experience. However, the value being close to the threshold indicates a possible weak relationship, where victim experience may slightly influence trust levels, but not in a strong or consistent manner.

4. Legal awareness and paranoia

The ANOVA results show a p-value of **0.507**, which is far greater than 0.05. This indicates that there is no statistically significant relationship between legal awareness and

feelings of paranoia. In other words, differences in legal awareness levels do not meaningfully affect how paranoid individuals feel about cyber threats.

5. **Education and practical security**

The p-value is approximately **0.571**, which is also much higher than 0.05. This indicates that there is no statistically significant difference in practical security behaviors across different education levels, suggesting that educational qualification does not strongly influence how individuals implement cybersecurity practices.

Conclusion:

In conclusion, the ANOVA analysis across different worksheets shows that among all the variables studied, only risky behavior has a statistically significant impact on protection levels, while other variables such as age, victim experience, legal awareness, and education do not show significant differences in their respective outcomes. This suggests that behavioral factors play a more important role than demographic or awareness-based factors in influencing cybersecurity practices, and therefore, efforts to improve cybersecurity should focus more on reducing risky behavior rather than relying solely on increasing awareness or education.

Conclusion

In summary, this paper demonstrates how cybercrime awareness, behavior, and victimization trends work within the Indian internet user community. The rapid growth of the digital technologies sector has contributed to the increased use of various cyber solutions but has also left users vulnerable to numerous cyber threats, thereby increasing the importance of cybersecurity.

According to the findings obtained, awareness works as an effective but limited factor. According to statistical data, it is linked to improved behavior and lower rates of victimization, and encourages victims to report cyber crimes. However, based on the analysis of correlations and ANOVA, awareness has little effect on the perception of cyber dangers and risky behavior of users. Many individuals continue to take unsafe actions even though they know about potential cyber threats.

Moreover, age, gender, and even education (sometimes) do not necessarily affect cybersecurity practices or being a victim of cybercrime. On the contrary, behavioral issues, especially high-risk online activities, tend to play a more critical role in affecting cybersecurity outcomes. Furthermore, the weak correlation between trust in law enforcement and reporting behavior highlights wider systemic problems, such as inadequate participation in reporting cyber incidents and low institutional efficiency.

As for the regression model, it supports the abovementioned observations, revealing awareness and previous experience as predictors of victimization and reporting behavior, while also suggesting that there is still much variation left unexplained by the current dataset, implying the existence of other variables outside the dataset.

To summarize, the findings suggest that cybersecurity cannot be achieved through awareness alone, nor is it a problem confined to one's knowledge level or demographic background; rather, it encompasses various factors, such as risky behavior, perception, and systemic barriers. Thus, policymakers must shift from relying solely on awareness campaigns to promoting behavioral change, skills development, and institutional trust building in order to ensure a safer cyber environment in the future.

Appendix

QUESTIONNAIRE:

Section A – Personal Information

1. Age Group:

- Below 18
- 18–25
- 26–35
- 36–50
- Above 50

2. Gender:

- Male
- Female
- Other
- Prefer not to say

3. Educational Qualification:

- School student
- College student
- Graduate
- Postgraduate
- Other (please specify): _____

4. Occupation:

- Student
- Business person/Self-employed
- Working professional/Employee
- Homemaker
- Other: _____

Section B – Online Habits and Device Use

5. How often do you use the Internet?

- Rarely (less than 1 hour per week)
- Occasionally (a few times a week, 1–5 hours total)
- Daily – Light use (less than 3 hours per day)
- Daily – Moderate use (3–6 hours per day)
- Heavy use (more than 6 hours per day / almost all day)

Section C – Cybercrime Awareness and Knowledge?

6. How familiar are you with the term "cybercrime"?

- I've never heard of it
- I've heard of it but don't know much
- I understand it fairly well
- I know a lot about it

7. Where did you first learn about cybercrime?

- Social media
- News/media
- Government campaigns
- School/College
- Friends/Family
- Other: _____

8. Which of the following do you think are examples of cybercrime? (Select all that apply)

- Hacking into someone's account
- Online fraud or phishing
- Posting fake news
- Cyberbullying
- Downloading movies illegally
- None of the above

9. How familiar are you with the following types of cyber threats?
(1 = Not Familiar, 5 = Very Familiar)

- Phishing: 1 2 3 4 5
- Malware: 1 2 3 4 5
- Identity Theft: 1 2 3 4 5
- Ransomware: 1 2 3 4 5
- Deepfakes / AI-based Scams: 1 2 3 4 5
- Online Financial Fraud (e.g., UPI or card scams): 1 2 3 4 5
- Social Media Hacking / Impersonation: 1 2 3 4 5
- Cyberbullying / Online Harassment: 1 2 3 4 5
- Data Breaches / Information Leaks: 1 2 3 4 5
- Online Shopping / E-commerce Scams: 1 2 3 4 5

10. Are you aware of India's cybercrime laws (like the IT Act, 2000) and the official reporting channels (Helpline 1930 or cybercrime.gov.in)?

- Aware of both
- Aware of only one
- Heard of them but not sure
- Not aware

Section D – Digital Payments and Security

11. Do you use online or digital payment methods (e.g., UPI, Paytm, Google Pay, Net Banking)?
- Yes
- No
- Which digital payment platforms do you use most frequently?
- UPI (PhonePe, Google Pay, Paytm, etc.)
- Debit/Credit Cards
- Net Banking
- Mobile Wallets
- Others (please specify): _____

12. How safe do you feel while making digital payments?
(1 = Very unsafe, 5 = Very safe)
1 2 3 4 5

Section E – Experience with Cybercrime and Digital Frauds

13. Have you or someone you know ever been a victim of cybercrime (online scam, identity theft, hacking, fake job scams, etc.)?
- Yes, I have personally been a victim
- Yes, someone I know has been a victim
- No

14. If yes, what type of cybercrime was involved? (Select all that apply)
- Phishing or scam messages
- Online shopping scam
- Social media or account hacking
- Financial fraud or UPI scam
- Cyberbullying or online harassment
- Fake job or lottery scam
- Data leak or identity theft
- Other: _____

15. If you ever faced a cybercrime incident, how did you respond and what was the outcome?
- Reported it to police/cybercrime portal and received help
- Reported it to police/cybercrime portal but got no help
- Reported it to the platform (e.g., bank, social media) and issue was resolved
- Did not report as I didn't know where to report
- Did not report as I didn't think it was serious

Section F – Online Safety Practices

16. Which of the following measures do you use for online security? (Select all that apply)

- Strong and unique passwords
- Two-step (multi-factor) authentication/verification
- Antivirus software
- Regular software updates
- Backing up devices
- Using a VPN
- Reviewing privacy settings
- Avoiding suspicious emails/links
- Changing passwords frequently
- None of the above

17. Do you use the same password for multiple accounts or rely on your web browser to save or create passwords?

- Yes
- No

18. How many times have you actually clicked on unknown links and attachments?

- Never
- Once or twice
- A few times (3–5 times)
- Many times (more than 5)
- Not sure / don't remember

Section G – Attitudes, Perceptions, and Reporting

19. How serious do you think the problem of cybercrime is in India today?
(1 = Not serious, 5 = Extremely serious)
1 2 3 4 5

20. In your opinion, which group is most vulnerable to cybercrime?

- Teenagers / Students
- Young working professionals
- Middle-aged individuals
- Elderly people
- Small business owners / entrepreneurs
- Corporate employees
- Government employees
- All groups are equally vulnerable

21. Which online activity do you think is most susceptible to cyber attacks? (Select all that apply)
- Online banking
- Online shopping
- Social media
- Email communication
- Downloading files/software
- Online gaming

22. How do you usually learn about cyber safety tips?
- Social media campaigns
- News/media
- Government awareness drives
- Educational institutions
- Friends/family
- Other: _____

23. To what extent do you agree with the following statement:
"Cybercrime has increased significantly in the last 3 years."
(1 = Strongly disagree, 5 = Strongly agree)
1 □ 2 □ 3 □ 4 □ 5 □

24. How likely do you think it is that you could become a victim of cybercrime?
(1 = Very unlikely, 5 = Very likely)
1 □ 2 □ 3 □ 4 □ 5 □

25. How much trust do you have in law enforcement agencies to handle cybercrime effectively?
(1 = No trust, 5 = Complete trust)
1 □ 2 □ 3 □ 4 □ 5 □

Section H – Prevention, Training, and Future Needs

26. Would you participate in a cybersecurity awareness workshop if offered?
- Yes
- No
- Maybe

27. Cyber safety should be included as a compulsory part of the school/college curriculum.
(1 = Strongly Disagree, 5 = Strongly Agree)
1 □ 2 □ 3 □ 4 □ 5 □

28. What is the most effective way to spread cybercrime awareness?
- Social media campaigns
- Educational programs
- Government ads
- Influencer-led drives
- Other: _____

29. What additional measures do you think should be taken to reduce cybercrime?

BEHIND THE REPORT

RESEARCH AND EDITORIAL DIRECTORS

Amishi Sharma

Manjari Garg

TEAM MEMBERS

Anikeit Gupta

Anshika Garg

Hiten Chauhan

Pratyaksh Kumar Bhatia

Suhani Bhati

Contact Us
Email: vittshala@srcc.du.ac.in
Website: https://www.vittshalasrcc.in/