Navigating The Digital Realm: A Comprehensive Study On The Awareness, Perception, And Legal Landscape Of Cybercrime And Cyber Law In India

Alampally Vijay Saradhi[1*], Dr Ashok Ruprao Yende[2]

[1*]Research Scholar, Bir Tikendrajit University
[2]Research Supervisor, Bir Tikendrajit University

***Corresponding Author:** Alampally Vijay Saradhi
*Research Scholar, Bir Tikendrajit University

ABSTRACT

Cybercrime has emerged as a significant threat in the digital age, necessitating a thorough investigation into the awareness and understanding of individuals, organizations, and government entities regarding cyber law. This article presents a detailed study conducted in Telangana, India, employing a descriptive research method. The research design encompasses both primary and secondary data collection, with a focus on surveying 110 respondents through a structured questionnaire. The study aims to shed light on the current level of awareness about cybercrime and cyber law, exploring perceptions and understanding among stakeholders.In the pursuit of comprehensive insights, secondary data is gathered from articles, journals, and websites, providing a broader context for the primary findings. The research methodology incorporates statistical tools such as frequency and percentage analysis, along with visualization tools like charts, to interpret the collected data effectively. The convenience sampling technique is employed to select participants, acknowledging the limitations and ethical considerations inherent in the study. The article also emphasizes the importance of raising awareness and promoting compliance with cyber law, proposing measures for enhancing education and collaboration among diverse stakeholders.The study not only contributes to the existing literature on cybercrime but also provides practical implications for policymakers, law enforcement agencies, and educational institutions. By examining the level of awareness, perceptions, and the legal landscape in Telangana, this research aims to pave the way for proactive measures to mitigate cyber threats and enhance cybersecurity practices in the digital ecosystem.

Keywords: Cybercrime awareness, cyber law, visualization tools, cybersecurity, etc.

I. INTRODUCTION

The ubiquity of digital technologies has ushered in an era of unprecedented connectivity, transforming the way we live, work, and communicate. However, this technological revolution has also given rise to the ominous specter of cybercrime, posing substantial threats to individuals, organizations, and governmental entities. In the bustling city of Telangana, India, a comprehensive study has been undertaken to delve into the levels of awareness and understanding of cybercrime and cyber law. This investigation seeks to explore the nuances of how various stakeholders in Telangana perceive and grapple with the complexities of cyber threats and legal frameworks in the digital landscape.

As the digital frontier continues to expand, the need for heightened awareness and effective legal mechanisms to combat cybercrime becomes paramount. The study aims to unravel the intricacies of the prevailing cyber ecosystem in Telangana, shedding light on the specific challenges faced by the city's residents, businesses, and government bodies. Beyond merely assessing awareness levels, the research endeavors to offer valuable insights into the perception of individuals regarding cyber threats and the legal recourse available to them. By understanding the specific dynamics of the local context, the study endeavors to inform strategic initiatives that can fortify cybersecurity measures and foster a more resilient digital environment.

The significance of this study extends beyond academic curiosity; it underscores the urgency for collaborative efforts between policymakers, law enforcement agencies, and the public at large. "Cybersecurity is a shared responsibility, and this research aims to contribute to the collective understanding of the challenges posed by cyber threats in Telangana." Through this exploration, the article aims to advocate for proactive measures, educational initiatives, and collaborative strategies that can fortify the city's defenses against the evolving landscape of cybercrime.

II. REVIEW OF LITERATURE

Jigar Shah (2016) Centres on uncovering the answers to concerning inquiries such as, ‘Is the internet user truly cognizant of their susceptibility to diverse cyber offences?’If netizens are knowledgeable about cybercrimes, to what degree are they informed? If they are not aware, what steps may be taken to enhance their awareness and keep them updated? The study proposed a conceptual framework elucidating the methods for promoting and executing awareness initiatives among internet users about cybercrimes.

Animesh Sarmah, Roshmi Sarmah, and Amlan Jyoti Baruah, (2017) The emergence and widespread use of novel technologies have led to a surge in cybercriminal activities in recent years. Cybercrime poses significant challenges to humanity. Safeguarding against cybercrime is an essential component for the societal, cultural, and security dimensions of a nation. The Indian government has implemented the IT Act of 2000 to address cybercrimes. The Act provides further amendments to the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891, and the Reserve Bank of India Act, 1934. Cybercrime may originate from any area of the globe and cross national borders over the internet, leading to both technological and legal challenges in detecting and prosecuting these crimes. International collaboration, coordination, and cooperation among states are necessary to address cyber-crimes. The primary objective of this study was to disseminate knowledge about cyber-crime among the general populace. In conclusion, it is imperative to understand that cyber-crimes cannot be condoned in any way. If someone becomes a victim of a cyber-attack, please promptly come forward and file a report at the local police station. If the perpetrators are not held accountable for their actions, they will persist indefinitely.

Prashant Mali, J. S. Sodhi, Triveni Singh and Sanjeev Bansal (2018) This article has offered an overview of current perspectives on the difficulties posed by cybercrime. The analysis started by examining the current definitions of cybercrime and cyberwarfare, identifying two issues that required resolution. Initially, it was discovered that there is a lack of universally acknowledged delineation for either cybercrime or cyber warfare. This is a challenge since, in the absence of a mutually accepted definition, it becomes arduous to engage in meaningful discussions on the underlying matters or even identify instances of cyber warfare. The text contains findings from a survey involving 325 participants, which aimed to assess their perspectives on security concerns, their level of awareness, and their attitudes towards using relevant software. The findings reveal that although there is a superficial level of confidence, with respondents claiming to be aware of the risks and employing many necessary precautions, a more comprehensive analysis suggests that there are several areas where fundamental knowledge and understanding are lacking. While novice users often had significant difficulties, there was also a notable lack of understanding among users who considered themselves to be highly knowledgeable about the internet.

Kapila, Pallavi. (2020) The Internet, a global interconnection of loosely interconnected networks, has facilitated the transmission of data and information across many networks. In recent years, the transport of data and information across remote networks has raised significant concerns over security. Some individuals have used the internet for illicit purposes such as unauthorised intrusion into others' networks and engaging in frauds. The illegal behaviours associated with the internet are referred to as Cyber Crimes. Given the growing prevalence of online activities such as online banking and online shopping, this word has become commonplace in today's headlines. Hence, to halt and punish the perpetrators of cybercrime, the legislation known as ‘Cyber Law’ was implemented. Cyber Law refers to the legal framework that governs the Internet, Cyberspace, and related matters such as online security and privacy. Hence, with the aims in consideration, this chapter is segmented into many parts to provide a concise outline of cybercrime, the culprits behind it (hackers and crackers), diverse forms of cybercrimes, and the progression of cyber laws in India. The chapter provides more insight into the functioning of these regulations and the several preventative methods that might be used to counteract this ‘hi-tech’ crime in India. Keywords: Internet, Cybercrime, Cyberlaw, Cyberspace, Online security, Online privacy, High-tech crime, Hackers, Crackers, Unauthorised access.

Piyush Parwani, Priyanka Nikose, and Jagrati Rathor (2022) The primary objective of the research is to raise awareness among individuals about cyber-crime via the use of significant threats. Cybercrime refers to criminal activities that exploit computer systems or networks. It often results in damage to persons' security and financial well-being. The unauthorised disclosure of personal information raises significant privacy issues. Cybercrime is increasingly becoming a formidable danger to individuals, unlike anything seen before. Warren Buffet characterises cybercrime as the foremost predicament faced by humankind, presenting genuine hazards to our species.Various forms of cybercrimes exist. These include activities such as doxing, hacking, copyright infringements, cyberterrorism, and fraud. Despite the existence of legislation in several nations, efforts to eliminate cyber-crime have been ineffective. The study discusses the level of knowledge and understanding of cyber-crime among individuals, as well as the essential measures needed to eliminate it.
Jamuna et al (2023) In the present day, the significance of cybersecurity is equivalent to that of economic security. Similar to several other criminal activities, cybercrime is now seeing a rise in occurrence. Engaging in the act of using computers and the Internet for the purpose of unlawfully acquiring an individual's personal identification or introducing illicit or harmful software. Cybercrime poses significant harm to individuals as it involves the direct theft of their personal data, which undermines their reputation within society. Moreover, cybercrime has a substantial adverse impact on our society, economy, and businesses. In terms of society, cybercrime contributes to bullying, identity theft, cyberstalking, and cyber-defamation, thereby subjecting victims to highly distressing situations. The economy and business are impacted by cybercrime, with several instances of data theft and hacks targeting major corporations in recent years. Companies allocate substantial financial resources annually to safeguard their systems against any kind of cyber theft or unauthorised use of their information. Cybercrime not only has a financial impact on individuals, but it also has spiritual consequences. For instance, women who compromise their modesty by sharing photos of themselves online experience such spiritual harm. Furthermore, the spiritual development of today's teenagers is hindered by the prevalence of cyber activities, as many

teenagers engage in such behaviours excessively. And terminate their life by suicide and sadness. In order to safeguard the general population from cybercrime, many legislations have been enacted to address the issue of cybercrime prevention, such as the Information and Technology Act of 2000 and the Indian Penal Code of 1860.

III. OBJECTIVES OF THE STUDY

IV. RESEARCH METHODOLOGY

Research Design:

The study adopts a descriptive research design to elucidate the current state of awareness regarding cybercrime and cyber law. This approach allows for a detailed exploration of perceptions and insights.

Data Collection:

Primary Data: Primary data is gathered through survey and questionnaire techniques. A structured questionnaire is developed to capture the opinions and insights of the participants. The survey targets 110 respondents from Telangana city, selected through convenience sampling.

Secondary Data: Secondary data is sourced from diverse materials such as articles, journals, and websites. This data supplements the primary information and aids in contextualizing the study within existing literature and frameworks.

Sampling Technique:

The study employs a convenience sampling technique to select 110 respondents from Telangana city. This method is chosen for its practicality and efficiency in accessing a diverse range of participants.

Data Analysis:

Statistical tools, including frequency and percentage analysis, are applied to interpret the collected data. These tools provide a quantitative insight into the level of awareness and perception regarding cybercrime and cyber law.

Visualization Tools:

To enhance data interpretation, various charts will be utilized. Visual representations, such as graphs and charts, will be employed to present key findings, making the information more accessible and comprehensible.

Ethical Considerations:

Ethical standards will be strictly adhered to throughout the research process. Participants will be informed about the purpose of the study, and their consent will be obtained. The confidentiality of respondents will be maintained, ensuring the privacy and integrity of the gathered data.

Limitations:

It is essential to acknowledge the limitations of the study, including the reliance on convenience sampling, potential biases in self-reported data, and the geographical constraint to Telangana city. These limitations will be considered in the interpretation of results.

Validity and Reliability:

To ensure the validity and reliability of the study, rigorous data collection and analysis procedures will be followed. The research instruments will be carefully designed, and the findings will be cross-verified to enhance the credibility of the results.

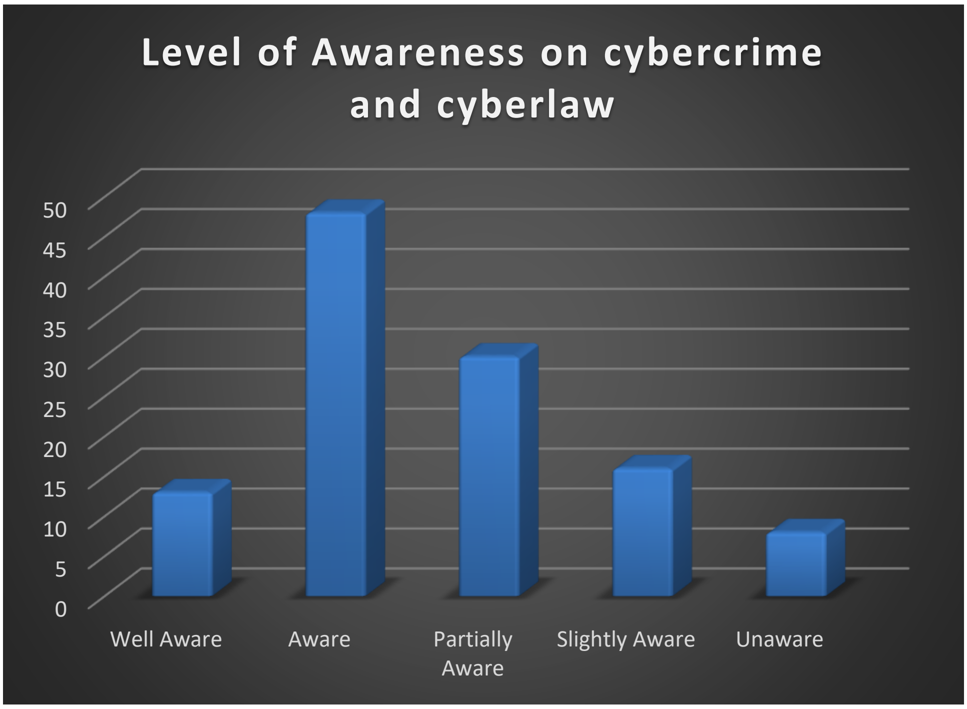
V. ANALYSIS AND INTERPRETATIONS

The data collected from various respondent have to analysis for the drawing conclusion. The data collected is presented in the form of charts and tables. A brief description of analysis and interpretation are given below:

Table 1: Level of Awareness on cybercrime and cyberlaw.

Particulars	Frequency	Percentage
Well Aware	13	11.8%
Aware	48	43.6%
Partially Aware	30	27.7%
Slightly Aware	16	14.5%
Unaware	8	7.3%
Total	**110**	**100.00**

The collected data on the level of awareness regarding cybercrime and cyberlaw has been meticulously analyzed to draw meaningful conclusions. Table 1 presents a breakdown of respondents based on their awareness levels. "The majority of participants fall into the ‘Aware’ category, constituting 43.6% of the sample, indicating a considerable level of understanding among the surveyed population." The data reveals that 11.8% are ‘Well Aware,’ suggesting a smaller but noteworthy proportion possess a higher degree of awareness. In contrast, 27.7% are categorized as 'Partially Aware,' and 14.5% as 'Slightly Aware,' indicating varying levels of knowledge among participants. A smaller percentage, 7.3%, falls under the 'Unaware' category, highlighting the existence of a segment with limited awareness.



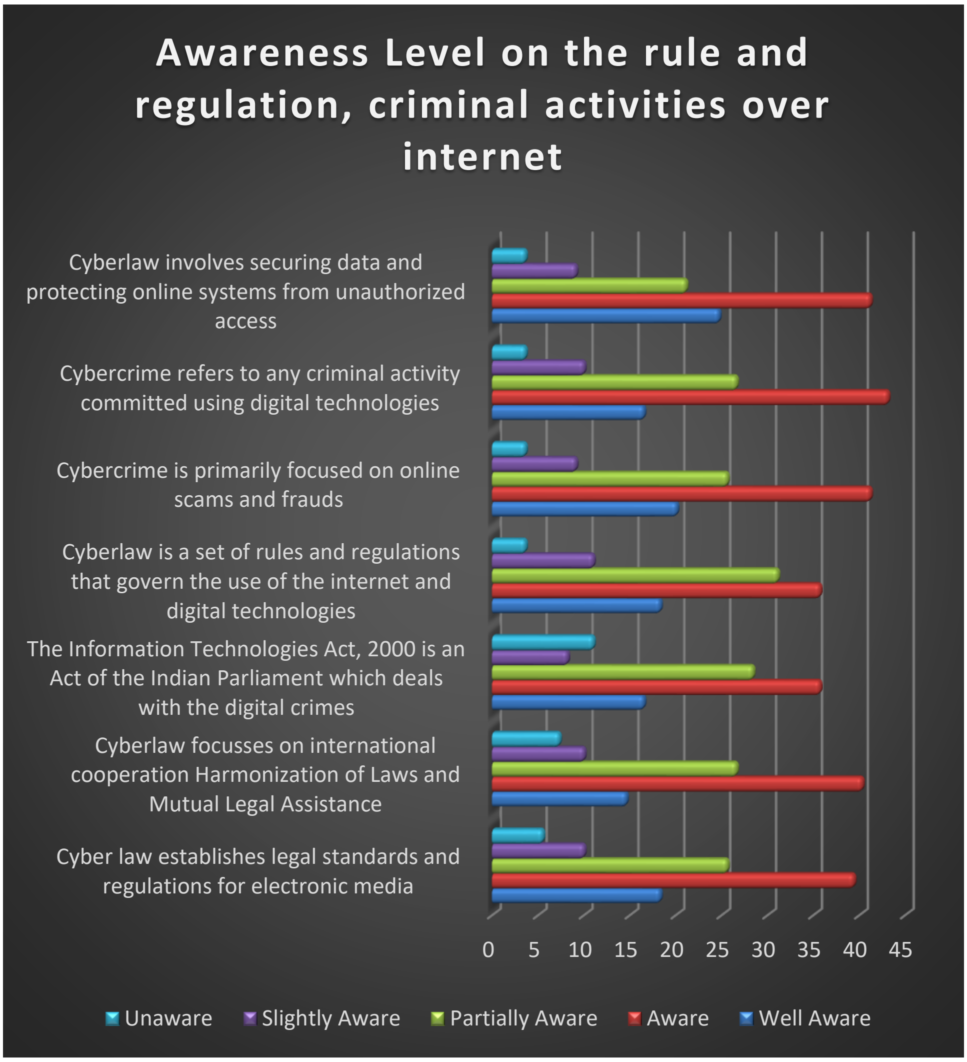
To provide a visual representation of the data, the findings have been translated into a chart format, aiding in a more accessible comprehension of the distribution. The results underscore the need for targeted educational initiatives and awareness campaigns to bridge gaps in understanding and enhance overall awareness regarding cyber threats and legal frameworks.

This table's significance extends beyond a mere enumeration of frequencies; it serves as a foundational component for understanding the landscape of cyber awareness among the surveyed population. As policymakers, educators, and stakeholders seek to address the challenges posed by cybercrime, insights from this analysis can guide the development of targeted interventions and strategies to bolster awareness and foster a more digitally resilient community.

Table 2: Awareness Level on the rule and regulation, criminal activities over internet

Particulars	Well Aware	Aware	Partially Aware	Slightly Aware	Unaware
Cyber law establishes legal standards and regulations for electronic media	18.3	39.4	25.6	10	5.5
Cyberlaw focusses on international cooperation Harmonization of Laws and Mutual Legal Assistance	14.6	40.3	26.6	10	7.3
The Information Technologies Act, 2000 is an Act of the Indian Parliament which deals with the digital crimes	16.5	35.7	28.4	8.2	11
Cyberlaw is a set of rules and regulations that govern the use of the internet and digital technologies	18.3	35.7	31.1	11	3.6
Cybercrime is primarily focused on online scams and frauds	20.1	41.2	25.6	9.1	3.6
Cybercrime refers to any criminal activity committed using digital technologies	16.5	43.11	26.6	10	3.6
Cyberlaw involves securing data and protecting online systems from unauthorized access	24.7	41.2	21.1	9.1	3.6

Table 2 provides a nuanced perspective on the awareness levels of respondents regarding rules and regulations related to cyber law and criminal activities over the internet. The data, gathered from a diverse group of participants, has been categorized into different levels of awareness.



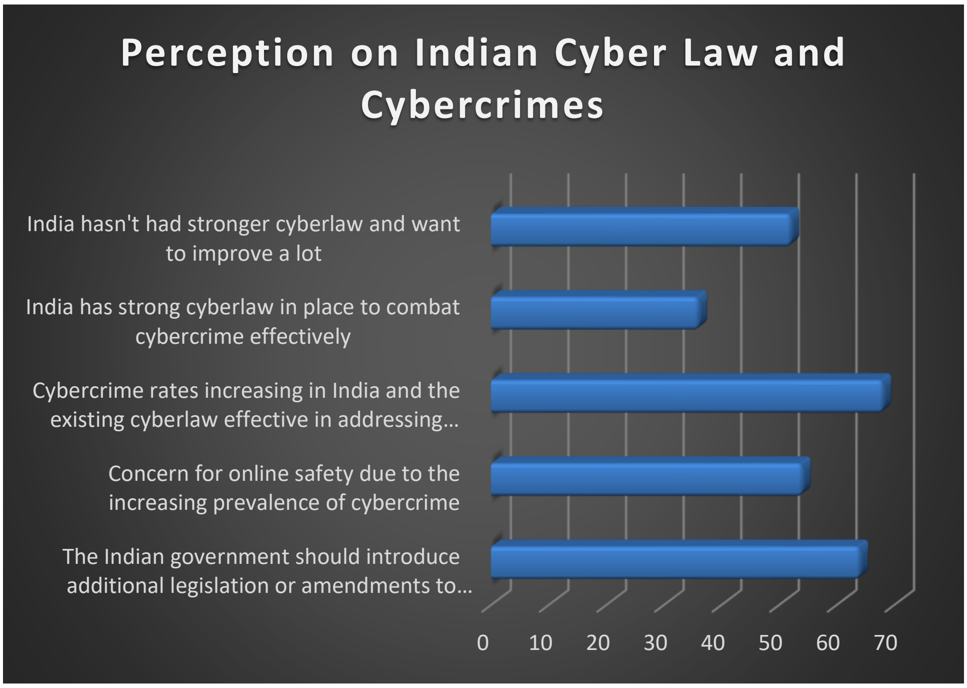
The findings reveal that a substantial portion of respondents demonstrates a commendable level of awareness across various aspects. Notably, 39.4% are 'Aware' that cyber law establishes legal standards and regulations for electronic media, with an additional 18.3% categorized as 'Well Aware.' A similar trend is observed in the awareness of international cooperation and harmonization of laws, where 40.3% fall under the 'Aware' category.The Information Technologies Act, 2000, which deals with digital crimes, is recognized by 35.7% of respondents, while 28.4% are categorized as 'Partially Aware.' Additionally, there is a strong awareness that cyber law involves securing data and protecting online systems from unauthorized access, with 24.7% falling under the 'Well Aware' category.

The data indicates varying levels of awareness across different aspects of cyber law and criminal activities over the internet. This nuanced understanding is crucial for tailoring educational initiatives and interventions that address specific gaps in awareness. The findings from Table 2 contribute valuable insights for policymakers, educators, and organizations seeking to enhance awareness and understanding of cyber law among the surveyed population.

Table 3: Perception on Indian Cyber Law and Cybercrimes

Particulars	**Frequency**	**Percentage**
The Indian government should introduce additional legislation or amendments to existing cyberlaw	64	57.8
Concern for online safety due to the increasing prevalence of cybercrime	54	49.5
Cybercrime rates increasing in India and the existing cyberlaw effective in addressing these issues	68	62.4
India has strong cyberlaw in place to combat cybercrime effectively	36	33
India hasn't had stronger cyberlaw and want to improve a lot	52	47.7
Total	**110**	**100.00**

Table 3 delves into the perceptions of respondents regarding Indian Cyber Law and Cybercrimes.



The data, collected from a diverse group of participants, provides valuable insights into their opinions and sentiments on various aspects related to cyber legislation and its effectiveness in addressing emerging challenges.A substantial 57.8% of respondents express the view that the Indian government should introduce additional legislation or amendments to existing cyber law. This suggests a prevalent belief among the surveyed population in the need for continuous evolution and reinforcement of legal frameworks to keep pace with the dynamic landscape of cyber threats.

Concerns for online safety due to the increasing prevalence of cybercrime are evident, with 49.5% of respondents expressing unease. This underscores the growing awareness and sensitivity among individuals regarding the potential risks associated with digital activities.A notable 62.4% of respondents believe that cybercrime rates are increasing in India, yet the existing cyber law is effective in addressing these issues. This dual perspective suggests a recognition of the evolving nature of cyber threats and an acknowledgment of the current legal framework's efficacy in managing these challenges.

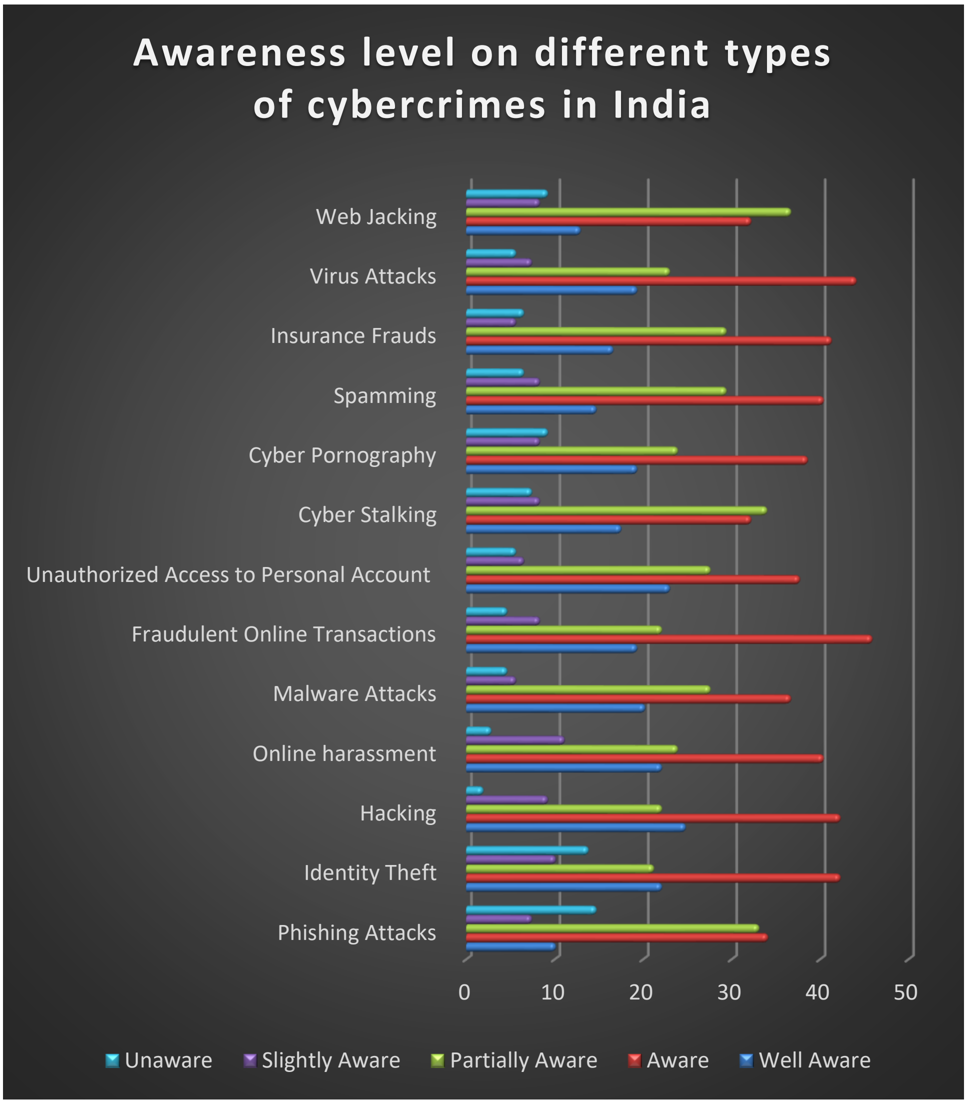
On the other hand, 33% of respondents believe that India already has a strong cyber law in place to combat cybercrime effectively. This perspective provides a contrasting viewpoint, indicating varying opinions on the adequacy of existing legal measures.Finally, 47.7% of respondents feel that India hasn't had stronger cyber law and express a desire for improvement. This viewpoint emphasizes the need for continual enhancement and strengthening of cyber laws to effectively counteract the evolving nature of cyber threats.

In summary, Table 3 encapsulates diverse perceptions regarding Indian Cyber Law and Cybercrimes, reflecting a nuanced understanding among respondents. These insights are crucial for policymakers and authorities as they navigate the landscape of cybersecurity legislation and work towards addressing the concerns and expectations of the public.

Table 4: Awareness level on different types of cybercrimes in India

Particulars	**Well Aware**	**Aware**	**Partially Aware**	**Slightly Aware**	**Unaware**
Phishing Attacks	10	34	33	7.3	14.6
Identity Theft	22	42.2	21.1	10	13.7
Hacking	24.7	42.2	22	9.1	1.8
Online harassment	22	40.3	23.8	11	2.7
Malware Attacks	20.1	36.6	27.5	5.5	4.5
Fraudulent Online Transactions	19.2	45.8	22	8.2	4.5
Unauthorized Access to Personal Account	22.9	37.6	27.5	6.4	5.5
Cyber Stalking	17.4	32.1	33.9	8.2	7.3
Cyber Pornography	19.2	38.5	23.8	8.2	9.1
Spamming	14.6	40.3	29.3	8.2	6.4
Insurance Frauds	16.5	41.2	29.3	5.5	6.4
Virus Attacks	19.2	44	22.9	7.3	5.5
Web Jacking	12.8	32.1	36.6	8.2	9.1

Table 4 provides a comprehensive overview of respondents' awareness levels concerning different types of cybercrimes in India. The data offers valuable insights into the varying degrees of familiarity with specific cyber threats, shedding light on the knowledge base of the surveyed population.Phishing Attacks emerge as a relatively well-understood concept, with 34% of respondents categorized as ‘Aware’ and 33% as ‘Partially Aware.’ This suggests a reasonable awareness of this prevalent form of cybercrime among the surveyed individuals.



Identity Theft and Hacking exhibit similar awareness patterns, with significant proportions falling under the ‘Aware’ category (42.2% and 42.2%, respectively). The findings suggest that these more complex cybercrimes are reasonably well-recognized by the respondents.Online Harassment, Malware Attacks, and Fraudulent Online Transactions reveal diverse awareness levels. While Online Harassment and Fraudulent Online Transactions show substantial awareness (40.3% and 45.8% respectively), Malware Attacks display a more balanced distribution across awareness categories.

Unauthorized Access to Personal Accounts, Cyber Stalking, and Cyber Pornography highlight mixed awareness levels, with varying proportions falling under different categories. These findings underscore the nuanced understanding respondents have regarding these specific cyber threats.Spamming, Insurance Frauds, Virus Attacks, and Web Jacking exhibit diverse patterns of awareness. Notably, Virus Attacks and Insurance Frauds display a higher percentage of respondents categorized as ‘Aware,’ indicating a relatively advanced awareness level regarding these cyber threats.

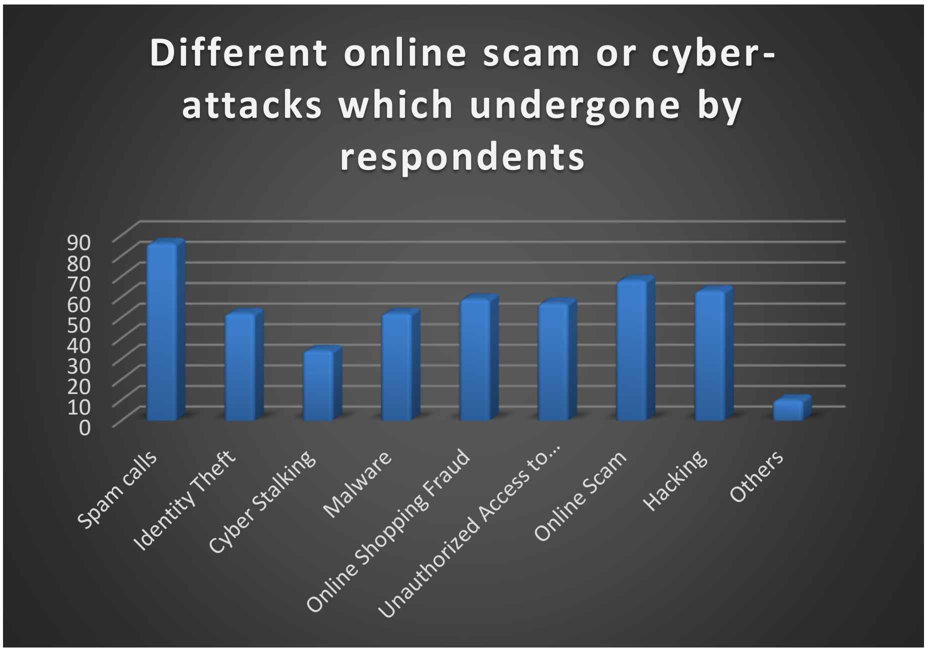
In summary, Table 4 unveils a multifaceted landscape of awareness regarding different types of cybercrimes in India. The insights derived from this data can inform targeted educational campaigns and cybersecurity initiatives to bridge knowledge gaps and enhance overall awareness among the surveyed population.

Table 5: Different online scam or cyber-attacks which undergone by respondents

Particulars	Frequency	Percentage
Spam calls	86	78.2
Identity Theft	52	47.3
Cyber Stalking	34	30.9
Malware	52	47.3
Online Shopping Fraud	59	53.6
Unauthorized Access to your Personal Data	57	51.8

Online Scam	68	61.8
Hacking	63	57.3
Others	10	9.1
Total	**110**	**100.00**

Table 5 provides a comprehensive overview of different online scams or cyber-attacks undergone by respondents, offering insights into the prevalence of various threats in the digital landscape.



Online Scams emerge as a significant concern, with a substantial 61.8% of respondents indicating that they have undergone such experiences. This suggests a prevalent and impactful occurrence of online scams among the surveyed population.Online Shopping Fraud and Unauthorized Access to Personal Data closely follow, with 53.6% and 51.8% of respondents, respectively, reporting experiencing these cyber-attacks. These findings underline the challenges associated with online transactions and the protection of personal information in the digital realm.

Hacking and Spam Calls are reported by 57.3% and 78.2% of respondents, respectively, indicating a high incidence of these cyber threats. The ubiquity of spam calls points to a pervasive issue affecting individuals in their daily lives.Identity Theft, Malware, and Cyber Stalking exhibit significant percentages, with 47.3%, 47.3%, and 30.9% of respondents, respectively, reporting experiencing these cyber-attacks. These findings highlight the diverse range of threats individuals face in the digital space, from personal data breaches to malicious software infiltrations.While the category labelled as ‘Others’ reflects a lower percentage, the presence of such incidents at 9.1% underscores the existence of additional, perhaps less common, cyber-attacks not explicitly specified in the table.

In summary, Table 5 offers a comprehensive view of the cyber threats and online scams experienced by respondents. The high prevalence of certain categories, such as spam calls and online scams, emphasizes the need for robust cybersecurity measures and awareness campaigns to mitigate the impact of these digital threats on individuals and the broader online community.

VI. CONCLUSION

In conclusion, this comprehensive study on the awareness of cybercrime and cyber law in Bangalore, India, has provided valuable insights into the perceptions, experiences, and knowledge levels of individuals regarding the ever-evolving digital landscape. The findings from the research underscore the significance of addressing the multifaceted challenges posed by cyber threats and the imperative to enhance awareness and education on cyber law.The study revealed varying levels of awareness among respondents, with a notable proportion demonstrating a commendable understanding of cyber threats and legal frameworks. The prevalence of online scams, identity theft, hacking, and other cyber-attacks reported by the respondents emphasizes the urgency of bolstering cybersecurity measures and fortifying legal frameworks to protect individuals and organizations in the digital realm.

Respondents' perspectives on the need for additional legislation or amendments to existing cyber law, coupled with concerns about the increasing prevalence of cybercrime, highlight the demand for proactive measures. The study advocates for collaborative efforts among policymakers, law enforcement agencies, educational institutions, and the public to strengthen cybersecurity awareness, promote compliance with cyber law, and mitigate the impact of cyber threats.The nuanced insights provided by this research can inform targeted interventions, educational initiatives, and policy reforms. As the digital landscape continues to evolve, it is imperative to adapt and strengthen cybersecurity measures to safeguard individuals, organizations, and government entities. The findings from this study contribute to the collective understanding of cyber awareness in Bangalore and serve as a foundation for future research and strategic initiatives aimed at fostering a more resilient and secure digital ecosystem.

REFERENCES

1. Animesh Sarmah, Roshmi Sarmah, and Amlan Jyoti Baruah, (2017) A brief study on Cyber Crime and Cyber Law's of India. International Research Journal of Engineering and Technology (IRJET). Volume: 04 Issue: 06. e-ISSN: 2395 -0056, p-ISSN: 2395-0072. https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf
2. http://ccasociety.com/what-is-irc-crime/
3. http://searchsecurity.techtarget.com/definition/emailspoofing
4. http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html
5. https://cybercrime.org.za/definition
6. https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf
7. https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india
8. https://www.tutorialspoint.com/information_security_ cyber_law/introduction.htm
9. Jamuna, KV, Jaiswal, J., Santosh, S. & Baiju, S. (2023) A Study on People's Opinion on Awareness about Cybercrime in India. The International Journal of Indian Psychology ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print) Volume 11, Issue 3. https://ijip.in/wp-content/uploads/2023/07/18.01.026.20231103.pdf
10. Jigar Shah (2016) A Study of Awareness About Cyber Laws for Indian Youth. International Journal of Trend in Scientific Research and Development, Volume 1(1), ISSN: 2456-6470. https://core.ac.uk/download/pdf/266990702.pdf
11. Kapila, Pallavi. (2020). Cyber Crimes and Cyber Laws in India: An Overview. https://www.researchgate.net/publication/350107577_Cyber_Crimes_and_Cyber_Laws_in_India_An_Overview
12. Piyush Parwani, Priyanka Nikose, and Jagrati Rathor (2022) 'Awareness Regarding Cyber Crime among People' International Journal of Research Publication and Reviews, Vol 3, no 1, pp 944-947. https://ijrpr.com/uploads/V3ISSUE1/IJRPR2425.pdf
13. Prashant Mali, J. S. Sodhi, Triveni Singh and Sanjeev Bansal (2018) 'analyzing the awareness of cyber-crime and designing a relevant framework with respect to cyber warfare: an empirical study' International Journal of Mechanical Engineering and Technology (IJMET) Volume 9, Issue 2. pp. 110–124, Article ID: IJMET_09_02_012. https://iaeme.com/MasterAdmin/Journal_uploads/IJMET/VOLUME_9_ISSUE_2/IJMET_09_02_012.pdf
14. www.tigweb.org/actiontools/projects/download/4926.doc