

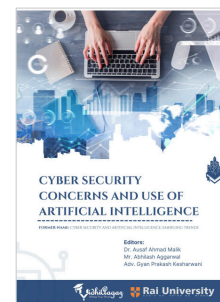
CHAPTER 38

Navigating the Cyber Frontier: Legal Challenges and Responses to Cybercrime in India

S. Indhu Dharshini and Jeyasri S.

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 315–334

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

S. Indhu Dharshini & Jeyasri S., *Navigating the Cyber Frontier: Legal Challenges and Responses to Cybercrime in India*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 315 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

S. Indhu Dharshini and Jeyasri S., ‘Navigating the Cyber Frontier: Legal Challenges and Responses to Cybercrime in India’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 315.

CHICAGO (17TH ED.)

Dharshini, S. Indhu, and Jeyasri S. “Navigating the Cyber Frontier: Legal Challenges and Responses to Cybercrime in India.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 315–334. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-38/>.

APA (7TH ED.)

Dharshini, S. I., & Jeyasri, S. (2024). Navigating the cyber frontier: Legal challenges and responses to cybercrime in India. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 315–334). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-38/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-38/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

NAVIGATING THE CYBER FRONTIER: LEGAL CHALLENGES AND RESPONSES TO CYBERCRIME IN INDIA

S. Indhu Dharshini⁷¹ and Jeyasri S.⁷²

ABSTRACT

Cybercrime has emerged as a significant threat in India affecting individuals, businesses and national security. With the rapid growth in digital technology and internet usage, there has been a surge in the number of cybercrimes such as hacking, identity theft, cyberbullying and data breaches. The legal framework for combating cybercrime in India revolves primarily around the Information Technology Act, 2000, which contains provisions to prevent and punish various cybercrimes. In addition, traditional laws such as the Indian Penal Code are also applicable to cybercrimes, including offences such as fraud, defamation and forgery. To stop and punish cyber criminals, "cyber laws" have been introduced. Cyber laws can be defined as the law of the Internet. It is the part of the legal system that deals with the Internet, cyberspace and other legal issues such as online security and online privacy. Studying this can help researchers, policymakers, legal professionals, and law enforcement agencies take proactive steps to combat this growing threat, protect individuals and organizations, and ensure a safe digital environment. The study aims to contribute to the enhancement of the legal framework, providing a data-driven approach to improving victim support and protection in the digital space.

Keywords: Cybercrime, digital space, victim challenges, legal framework, demographic factors, preventive reforms, cybercrime awareness.

BACKGROUND

The rise of the internet and the widespread use of digital technology have radically altered the way people interact, communicate, and do business as a result of the growing usage of digital technology and the internet. Although there are many advantages to these developments, they have also led to the emergence of cybercrime, a new category of criminal conduct. Cybercrime pertains to illicit actions that are enabled or carried out using computers, networks, and the Internet.

Cybercriminals use flaws in computer networks, systems, and online platforms to commit a range of criminal activities. Phishing, impersonation, identity theft, cyberbullying, child pornography, and domain name conflicts are a few of them. Cybercrime may have detrimental effects on people's finances, relationships, and mental health. These effects extend beyond individuals to include governments, businesses, and even national security. Policymakers and legal professionals may create strong legal frameworks to successfully tackle cybercrime by analysing these problems.

In the future, as cyber threats grow more sophisticated with advancements like AI and quantum computing, legal frameworks will need to adapt rapidly to address new challenges. Stronger international cooperation, real-time digital forensics, and evolving privacy laws will be crucial in ensuring a safer digital environment.

⁷¹ Student at Sastra Deemed To Be University, Thanjavur, Tamil Nadu, India.

⁷² Student at Sastra Deemed To Be University, Thanjavur, Tamil Nadu, India.

LITERATURE REVIEW

Cybercrime Trends and Patterns - This review examines various trends and patterns in cybercrime, focusing on types of cyber offenses, perpetrator behaviors, and technological advancements. It provides a comprehensive overview of cybercrime statistics. Legal Frameworks for Cybercrime Prevention - This literature review explores existing legal frameworks and policies designed to combat cybercrime. It analyzes how laws are implemented and their effectiveness in deterring cybercriminals. Technological Solutions to Cybercrime - This review focuses on technological solutions and advancements aimed at preventing cybercrime. It emphasizes software and hardware developments without considering how these measures impact victims or the necessity of victim feedback in creating effective technologies. Cybercrime and Social Media: A Review of Threats - This literature review addresses various threats associated with cybercrime in the realm of social media, such as phishing, hacking, and identity theft.

Perpetrator Motivations in Cybercrime - This review investigates the motivations behind cybercriminal behaviours, exploring factors such as financial gain, ideological beliefs, and psychological profiles. It offers valuable insights into why crimes occur. Cybersecurity Measures: Efficacy and Challenges - This literature review analyses various cybersecurity measures and their effectiveness in preventing cybercrime. It discusses institutional and organizational approaches. The Role of Law Enforcement in Cybercrime Investigation - This review explores the role of law enforcement agencies in investigating and prosecuting cybercrime. It focuses on procedural aspects and challenges faced by law enforcement.

RESEARCH PROBLEM

To analyse the challenges faced by victims, providing a more comprehensive view of legal issues in India from their perspective.

RESEARCH OBJECTIVES

1. To examine different types of cybercrime to gain a comprehensive understanding of the range of criminal activities carried out in the digital space.
2. To find out the awareness of internet users about cybercrime.
3. To propose preventive reforms and effective regulations to control cybercrime.

RESEARCH QUESTION

Whether demographic factors, such as age and gender, influence individuals' experiences with cybercrime, including their likelihood of reporting such incidents?

RESEARCH HYPOTHESIS

Demographic factors such as age and gender significantly influence individuals' experiences with cybercrime, impacting the likelihood of encountering cybercrime and reporting incidents.

RESEARCH METHODOLOGY

The Research Design is Empirical Research, Sample was the Population Aged between 20 to 50 irrespective of their gender & ethnicity.

The objectives of the study were to study the level of awareness amongst people, and to study the measures taken by people to prevent cybercrime.

The sample size consists of 122 general public opinions both males and females and the Sampling Method was Stratified Technique for this research. The data was collected from people all across India with the help of the Tools that is Google Forms, Questionnaire of 20 questions.

UNDERSTANDING THE CYBER CRIMES

Cybercrime refers to criminal activities carried out using digital technology, computer networks or the Internet. It involves the unauthorised use of information and communication technology to carry out illegal activities, exploit vulnerabilities or cause harm to individuals, organisations or society as a whole. Preventing and combating cybercrime requires strong cybersecurity measures, effective legislation and advances in technology and digital forensics.

It threatens an individual's privacy by disclosing or publishing their personal or confidential information online with the intention of damaging their reputation and causing physical or mental harm, directly or indirectly.

CATEGORIES OF CYBERCRIME

Cybercrime is not limited to a few types known to Internet users but they are constantly evolving with new strategies, posing challenges to stop them.

1. Crimes against individuals

Crimes that harm specific individuals. These crimes include harassment by email, online harassment, cyberbullying, dissemination of obscene material, defamation, copyright infringement, hacking, electronic message address theft, SMS theft, wiretapping, fraud and deception, child pornography, intimidation, denial of service, spoofing and fraud.

A) Cyber stalking

It means to create a physical threat that creates fear using computer technology such as the internet, e-mail, phones, text messages, webcam, websites or video.

B) Hacking:

It means unauthorised control/access over a computer system and an act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hack telecommunication and mobile networks.

C) Child Pornography:

It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

D) Assault by Threat:

refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

E) Cheating & Fraud:

It means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with a guilty mind which leads to fraud and cheating.

2. Crimes against Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents.

A) Cyber Squatting:

It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

B) Intellectual Property Crimes:

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

C) Cyber Vandalism:

Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

D) Transmitting Virus:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

E) Cyber Trespass:

It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

F) Identity theft

It is a form of fraud or simply deceit that is done by using the personal information of someone else whose information is not authorised to be used by someone other than him under the law. Section 66C of the Information Technology Act, 2000 provides for punishment for identity theft. It says if anyone fraudulently or dishonestly uses any electronic signature, password, or unique identification feature of

any other person, they are guilty of identity theft and liable for imprisonment of either description for a maximum of three years and a fine up to one lakh rupees.

3. Cybercrimes against Government

A) Possession of Unauthorized Information:

It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

B) Cyberterrorism:

Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

C) Distribution of pirated software:

It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

NEED FOR CYBERCRIME LAWS IN INDIA

- Cyberlaw is of particular importance in countries such as India, where the internet is used widely. In order to protect both individuals and organizations against cyber crime, the law was enacted. The cyberlaw allows other people or organizations to take legal action against someone if that person violates and breaks the provisions of the law.
- Cyberlaw may be required in the following circumstances:
- Due to the fact that all the transactions associated with stocks are now executed in demat format, anyone who is involved with these transactions is protected by cyber law in the event of any fraudulent transactions.
- Almost all Indian companies have electronic records. A company may need this law to prevent the misuse of such data.
- As a result of the rapid development of technology, various government forms are being filled out electronically, such as income tax returns and service tax returns. Anybody can misuse those forms by hacking government portal sites, and thus, cyberlaw is required under which legal action can be taken.

WHO ARE VICTIMS OF CYBERCRIME IN INDIA?

Defining victims of cybercrime in India presents challenges similar to those encountered in defining cybercrime itself. To understand the concept of a cybercrime victim in the Indian context, we can refer to guidelines such as the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985). According to this declaration, victims are individuals or groups who have

suffered harm—be it physical, mental, emotional, or economic—or experienced a significant violation of their fundamental rights due to acts or omissions that contravene criminal laws.

Two key aspects emerge from this definition within the Indian context. Firstly, the classification of a victim relies heavily on the nature of harm suffered. Victims can be seen as those affected both materially and non-materially by cybercrime. Secondly, victims can be categorized into two groups: direct victims—those who suffer directly from the cybercrime—and indirect victims, including family members or dependents of the direct victim. Although the primary focus is typically on direct victims, the definition may also encompass immediate relatives in relevant circumstances, particularly in cases involving emotional or psychological harm.

A significant case that illustrates the impact of cybercrime on victims in India is the Avinish Bajaj school porn case (2008). In this incident, a minor student was subjected to severe harassment after an intimate video was circulated online without consent. The case highlighted the devastating emotional and psychological toll on the victim, demonstrating the need for robust protections against such violations. The Supreme Court's decision underscored the importance of addressing the rights of victims in cases involving non-consensual content, emphasizing that victims should be treated with sensitivity and afforded legal recourse.

This case exemplifies the necessity of acknowledging and addressing the complexities surrounding victims of cybercrime in India, ensuring that both direct and indirect victims receive the support and justice they deserve.

A. Physical Impacts:

In addition to damaging assets like computer hardware or infrastructure, certain cybercrimes can lead to severe consequences for individuals, including physical harm and even loss of life. Cyberbullying, cyberstalking, and other forms of online harassment have been linked to serious psychological distress, which, in extreme cases, can lead to self-harm or suicide. Victims of cyberbullying, particularly vulnerable individuals such as teenagers or those already facing mental health challenges, may experience overwhelming feelings of isolation, depression, or helplessness, sometimes culminating in tragic outcomes like suicide.

These cyber-attacks not only affect mental health but can also push victims towards physical harm. For example, non-consensual dissemination of intimate images, often referred to as "revenge porn," can leave victims feeling violated and lead to severe psychological trauma, resulting in physical harm or even death in some cases.

Beyond the individual level, damage to physical infrastructure from cybercrimes, such as attacks on hospitals or emergency services, can disrupt essential services, potentially putting lives at risk. These cascading effects can impact not only victims directly targeted by cybercriminals but also broader segments of society, heightening the need for robust cybersecurity measures and support systems for victims.

B. Financial Impacts:

Cybercrime can cause substantial financial damage to both businesses and individuals. Even a single cyberattack can lead to significant financial losses. For instance, the 2017 WannaCry ransomware attack affected around 230,000 computers globally, resulting in an estimated financial loss of US\$4 billion. Additionally, the global cost of cybercrime is estimated to reach \$1 trillion annually, though these figures often reflect broader national economic impacts rather than the specific financial burden on individual victims.

In India, cybercrimes have also had serious financial repercussions. For example, the 2018 Cosmos Bank cyberattack resulted in a loss of nearly INR 94 crores after hackers infiltrated the bank's server and siphoned funds via fraudulent ATM transactions. Similarly, the Punjab National Bank scam, one of the largest frauds in Indian banking history, involved the misuse of the SWIFT system to illegally transfer INR 11,400 crores.

On a personal level, individuals in India are frequently targeted by phishing scams, identity theft, and online financial fraud, leading to significant monetary loss. These attacks often target vulnerable populations who may not have access to cybersecurity education, further exacerbating the financial burden on victims. As cybercriminals employ increasingly sophisticated methods, the financial toll on Indian businesses and individuals continues to rise, demanding stronger cybersecurity measures and legal frameworks to address the issue.

C. Psychological and Emotional Impacts:

Cybercrime can have profound psychological and emotional effects on individuals. Victims may experience a range of emotions, including anger, anxiety, fear, and a loss of confidence in technology. They often feel ashamed, vulnerable, or powerless, which can lead to depression. This is particularly true for victims of online abuse, such as cyberstalking, doxing, harassment, or the non-consensual dissemination of intimate images. Many victims internalize guilt and self-blame, compounding their psychological distress.

In India, several case laws highlight the emotional toll of cybercrime on victims. For instance, the landmark case of *Shreya Singhal v. Union of India* (2015) addressed the issue of Section 66A of the Information Technology Act, which was used to penalize offensive online messages. The Supreme Court ruled the provision unconstitutional, emphasizing the need to protect individuals from arbitrary online harassment while also recognizing the psychological impact that cyberbullying and online threats can have on victims.

Another relevant case is **Sakshi v. Union of India** (2004), where the Supreme Court recognized the need to protect minors from sexual abuse in the digital space, leading to more stringent laws against online harassment and exploitation. This case brought attention to the emotional trauma experienced by victims of such crimes, emphasizing the importance of providing psychological support and legal recourse.

Furthermore, in the case of *Sushmita v. State of Maharashtra* (2018), the victim of non-consensual sharing of intimate images sought justice, highlighting the severe emotional distress caused by the act.

The court's recognition of the victim's suffering underscored the need for comprehensive measures to address the psychological impact of cybercrimes.

These cases illustrate not only the legal framework surrounding cybercrime in India but also the importance of acknowledging and addressing the psychological and emotional impacts on victims, which can have lasting effects on their mental health and well-being.

D. Reputational Impacts:

In addition to financial losses, cybercrime can significantly harm reputations. At the organizational level, a cyber incident can tarnish a company's image, erode customer trust, damage public perception, and reduce business opportunities. For individuals, the exposure of private information during a cyberattack can severely damage their reputation, especially if the leaked information is sensitive or damaging.

In India, several high-profile cases illustrate the reputational impacts of cybercrime. For example, the 2018 data breach at the online food delivery service Zomato exposed the personal data of over 17 million users, including email addresses and hashed passwords.

This incident not only resulted in financial losses for the company but also raised concerns among customers regarding data security, leading to a decline in user trust and potentially impacting business opportunities.

Another notable case is the data breach involving the hotel chain Marriott International, which affected over 5 million Indian guests. The exposure of sensitive personal information raised serious questions about the company's cybersecurity measures and resulted in significant reputational damage, as customers began to doubt their data's safety with the brand.

On an individual level, incidents of doxing—where personal information is publicly disclosed without consent—can lead to severe reputational harm. For instance, the case of a prominent Indian actress whose private images were leaked online led to widespread media coverage and public scrutiny, impacting her personal and professional life.

This incident not only highlighted the severe emotional distress faced by the victim but also underscored the broader societal implications of reputational damage resulting from cybercrime. These examples demonstrate that the reputational impacts of cybercrime can be profound, affecting both organizations and individuals in India. The erosion of trust, damage to public perception, and the potential for lost business opportunities highlight the need for robust cybersecurity measures and proactive responses to incidents.

WHAT ARE THE NEEDS OF VICTIMS OF CYBERCRIME?

By all accounts, victims' needs can be diverse, as the impacts of cybercrime on them can range from material, such as financial loss, to non-material, including reputational damage and psychological and emotional distress. Some victims may have suffered financial loss and require compensation. When victims continue to experience the negative consequences of cybercrime, they may adopt a more punitive stance and seek to prosecute the offender. However, for others, there can be more pressing

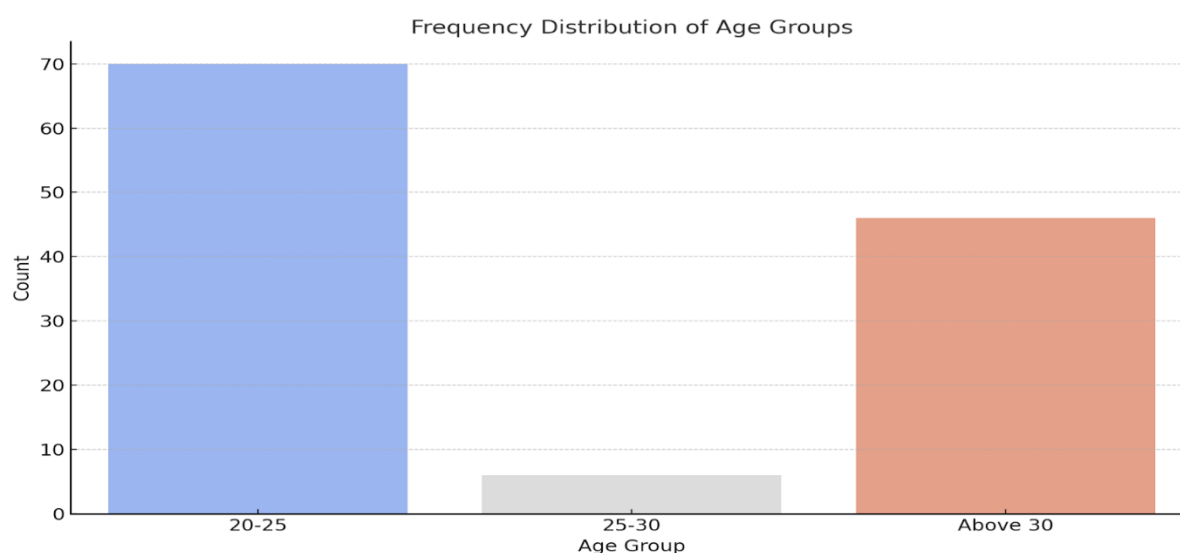
matters than retribution. These needs may include an apology, assistance and protection, recognition and condemnation of the harm, guarantees of safety, restoration to the situation preceding the cyber incident, prevention of the recurrence of the cybercrime, or participation in criminal proceedings.

In India, the needs of victims can also include immediate responses, such as the removal of illegal content posted online. For instance, in cases of cyberbullying or the non-consensual sharing of intimate images, victims may require urgent action to mitigate further harm and restore their dignity. Additionally, some victims may require responses that take into account their specific vulnerabilities and needs, such as psychological support or counseling services.

It is important to acknowledge that victimhood varies depending on various factors, including individual vulnerabilities, psychological perspectives, and age-related differences.

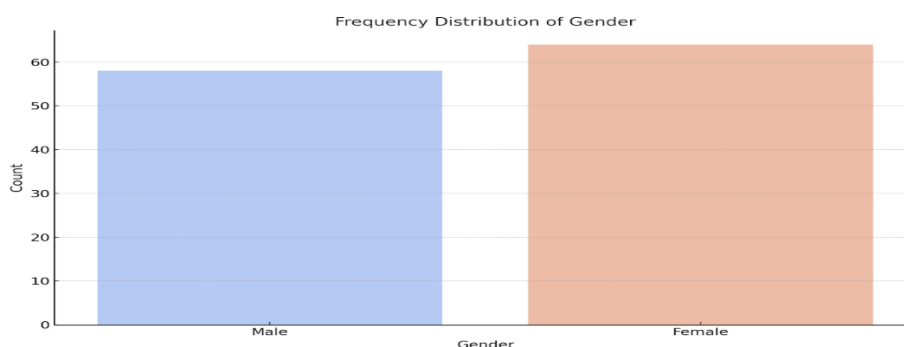
VISUALISATION OF DATA

1. Age



- The bar chart below represents the distribution of respondents across different age groups.
- The majority of the respondents (57%) fall within the **20-25 age group**. The next largest group is **Above 30** (38%), followed by a small portion of respondents aged **25-30** (5%).

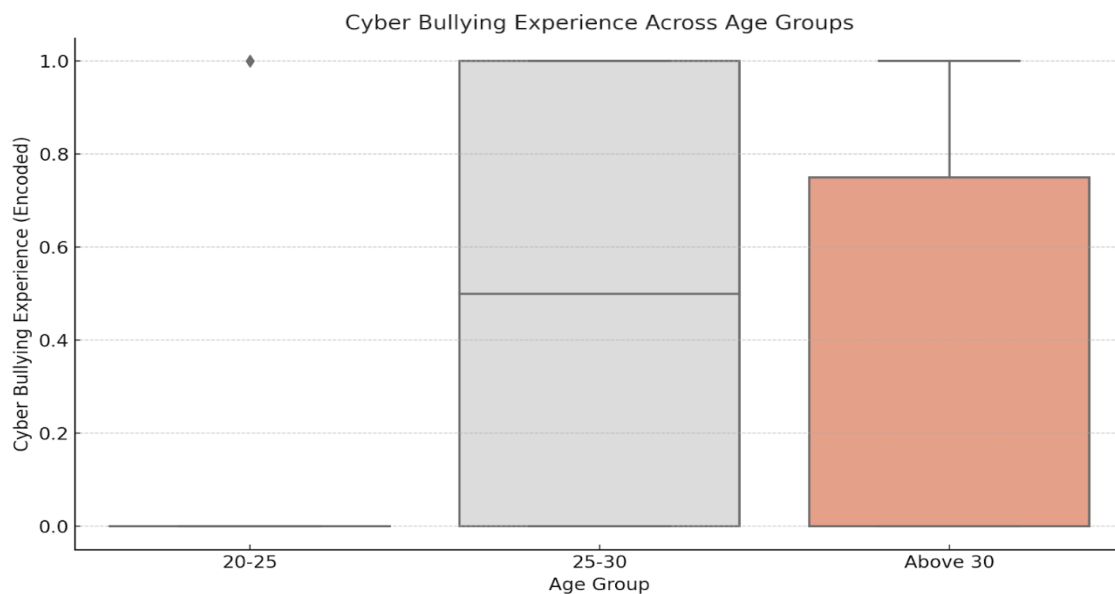
2. Gender



- The respondents are nearly evenly split between genders, with **52% female** and **48% male**.

Gender	No Cyberbullying	Yes Cyberbullying
Male	53	11
Female	43	15

3. Cyber Bullying Experience Across Age Groups

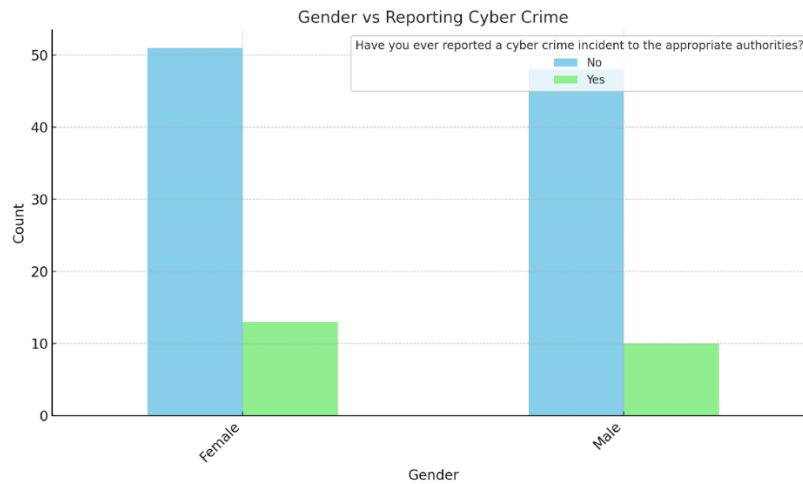


- About **21% of respondents** have experienced cyber bullying (mean value of 0.21 for the encoded data).
- The cross-tabulation analysis shows that individuals in the **20-25 age group** have reported the highest number of cyber bullying incidents. Out of the 70 respondents in this age group, 11 (16%) have experienced cyber bullying. In contrast, individuals **Above 30** report cyber bullying at a slightly higher rate (26%) compared to the other groups.

Age Group	No Cyber bullying	Yes Cyber bullying
20-25	59	11
25-30	3	3
Above 30	34	12

- Younger individuals (20-25) report more cyber bullying incidents in total, but the relative percentage is higher among respondents above 30.

4. Gender & Reporting Cyber Crime

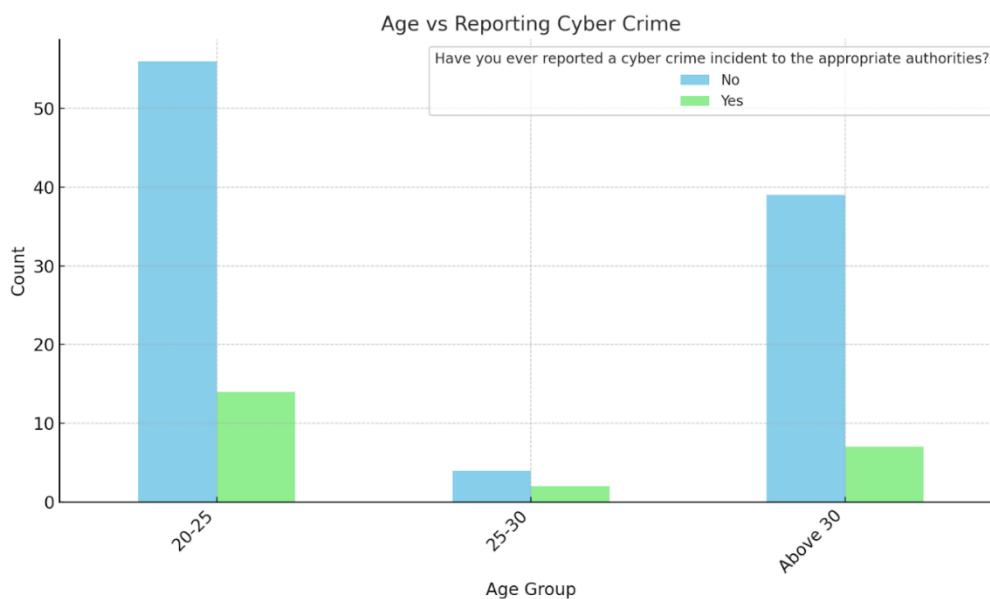


- About **19% of respondents** have reported cybercrimes to authorities
- The cross-tabulation indicates that **males** are slightly more likely to report cyber bullying than females. **15 males** (26%) reported experiencing cyber bullying, compared to **11 females** (17%).

Gender	No Report	Yes Report
Male	48	10
Female	51	13

- The analysis shows that **females** are slightly more likely to report cybercrimes than males. **13 females** (20%) reported cybercrimes, compared to **10 males** (17%).

5. Age & Reporting Cyber Crime



- This cross-tabulation helps us understand how the tendency to report cyber crimes varies by age group.

- The cross-tabulation reveals that **20-25 year-olds** are the most likely to report cyber crimes, with **14 individuals** (20%) having reported incidents. Individuals **Above 30** have a lower reporting rate (15%).

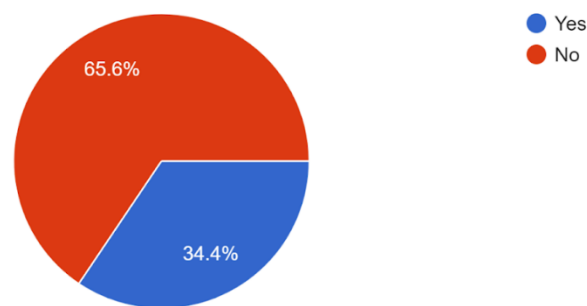
Age group	No Report	Yes Report
20-25	56	14
25-30	04	02
Above 30	39	07

- Younger individuals are more likely to report cyber crimes, possibly due to greater awareness or confidence in the reporting process.

6. Have you ever felt threatened or stalked online?

Have you ever felt threatened or stalked online?

122 responses

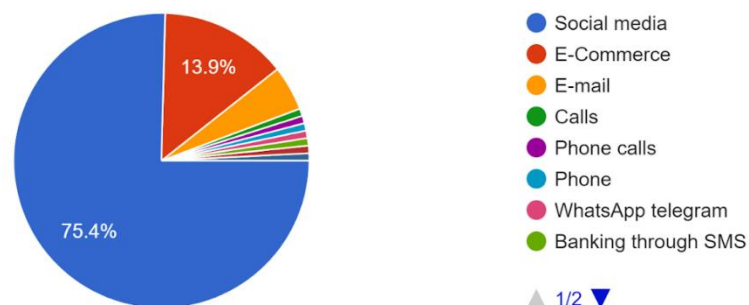


- 65.6% of respondents have never felt threatened or stalked online.
- 34.4% of respondents have felt threatened or stalked online.

7. What platforms do you believe are most at risk for cyber crimes?

What platforms do you believe are most at risk for cyber crimes?

122 responses

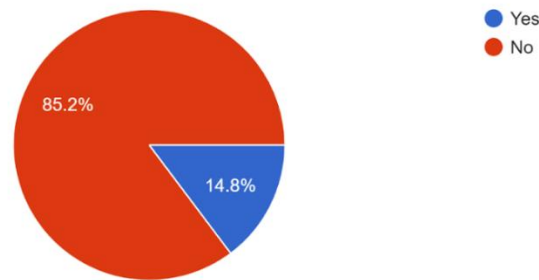


- 75.4% of respondents believe that social media platforms pose more risk for cyber crimes.

8. Have you ever been a victim of identity theft?

Have you ever been a victim of identity theft?

122 responses

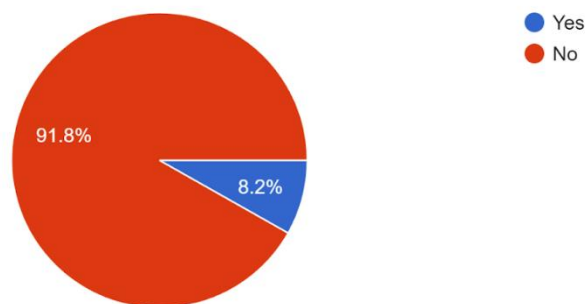


- 85.2% of respondents have never been a victim of identity theft.
- 14.8% have been a victim of identity theft.

9. Have you ever faced issues with domain name registration or ownership?

Have you ever faced issues with domain name registration or ownership?

122 responses

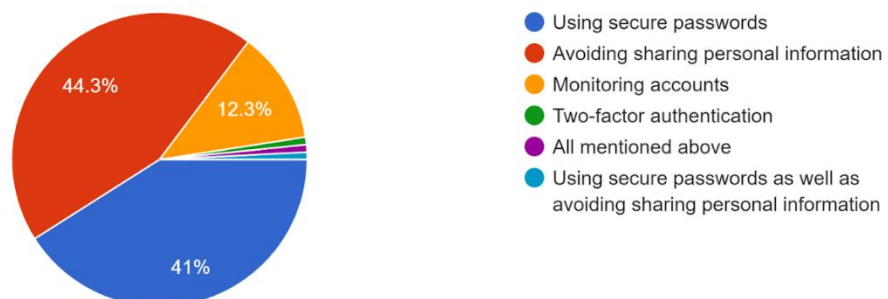


- 91.8% have never faced issues with domain registration or ownership.
- 8.2% have faced issues with domain registration or ownership.

10. What steps do you take to protect your personal information online?

What steps do you take to protect your personal information online?

122 responses



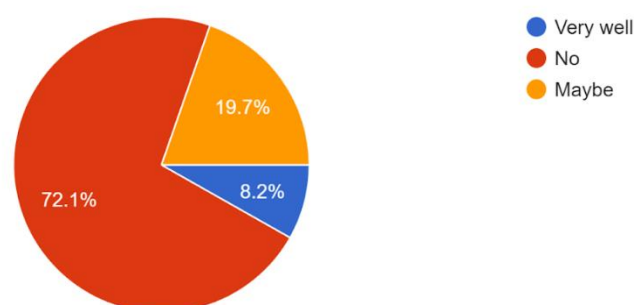
- 44.3% of respondents believe avoiding sharing personal information can protect their personal information online.
- 41% of respondents believe using secure passwords can protect their personal information online.

- 12.3% of respondents believe monitoring accounts can protect their personal information online.

11. Have you ever been a victim of cyber crime?

Have you ever been a victim of cyber crime?

122 responses

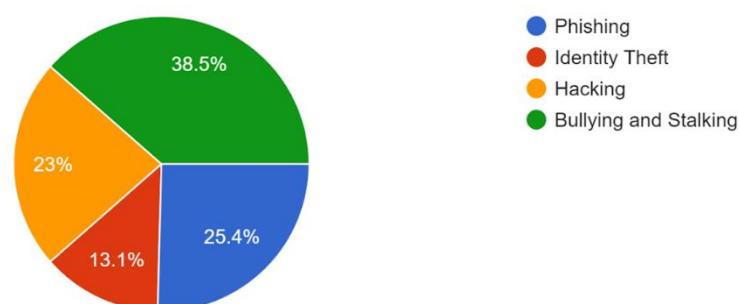


- 72.1% of respondents have not been a victim of cyber crime.
- 19.7% of respondents are not sure about it.
- 8.2% of respondents have been a victim of cyber crime.

12. Which of the following do you consider as the most common type of cyber crime?

Which of the following do you consider as the most common type of cyber crime?

122 responses

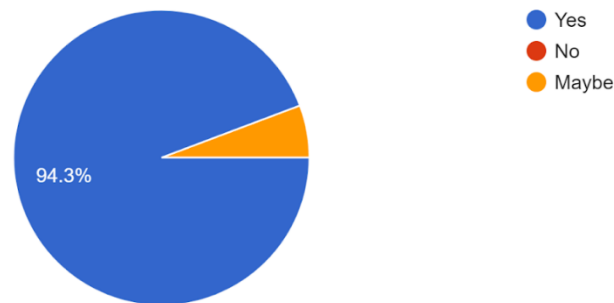


- 38.5% of respondents consider bullying and stalking as the most common type of cyber crime.
- 25.4% of respondents consider phishing as the most common type of cyber crime.
- 23% of respondents consider hacking as the most common type of cyber crime.
- 13.1% respondents consider identity theft as the most common type of cyber crime.

13. Do you believe cyber crime is increasing in today's digital world?

Do you believe cyber crime is increasing in today's digital world?

122 responses

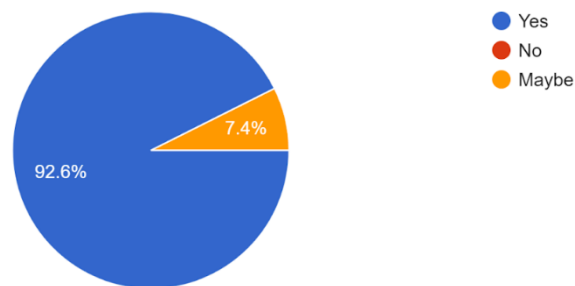


- 94.3% of respondents believe cyber crime is increasing in today's digital world.

14. Do you believe individuals should take more responsibility for protecting themselves from cyber crime?

Do you believe individuals should take more responsibility for protecting themselves from cyber crime?

122 responses

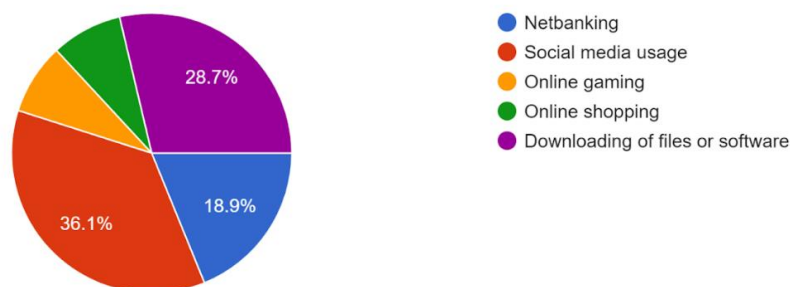


- 92.6% of respondents believe individuals should take more responsibility for protecting themselves from cyber crime.
- 7.4% of respondents are not sure about individuals should take more responsibility for protecting themselves from cyber crime.

15. Which of the following online activities do you consider the most vulnerable to cyber crime?

Which of the following online activities do you consider the most vulnerable to cyber crime?

122 responses



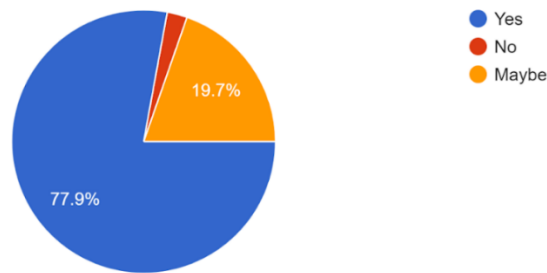
- 36.1% of respondents consider social media usage is the most vulnerable to cyber crime.

- 28.7% of respondents consider downloading files or software is the most vulnerable to cyber crime.
- 18.9% of respondents consider netbanking is the most vulnerable to cyber crime.

16. In your opinion, does cyber crime have a significant impact on individuals' daily lives?

In your opinion, does cyber crime have a significant impact on individuals' daily lives?

122 responses

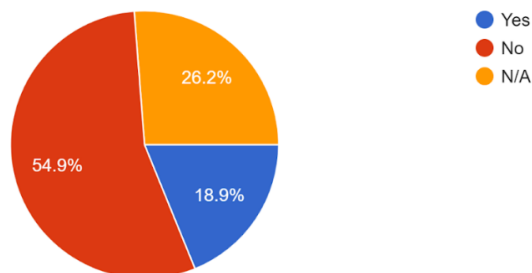


- 77.9% of respondents believe cyber crime has a significant impact on individual's daily lives.
- 19.7% of respondents are not sure about it.

17. Have you ever reported a cyber crime incident to the appropriate authorities?

Have you ever reported a cyber crime incident to the appropriate authorities?

122 responses

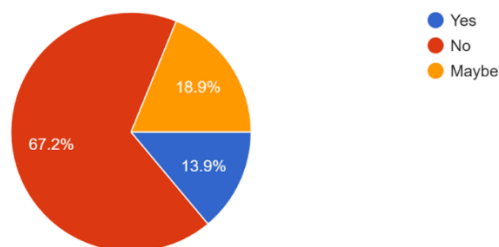


- 54.9% of respondents have never reported a cyber crime incident to the appropriate authority.
- 26.2% of respondents are not sure about it.
- 18.9% of respondents have reported a cyber crime incident to the appropriate authority.

18. Do you believe there is enough public awareness about the risks of cyber crime?

Do you believe there is enough public awareness about the risks of cyber crime?

122 responses

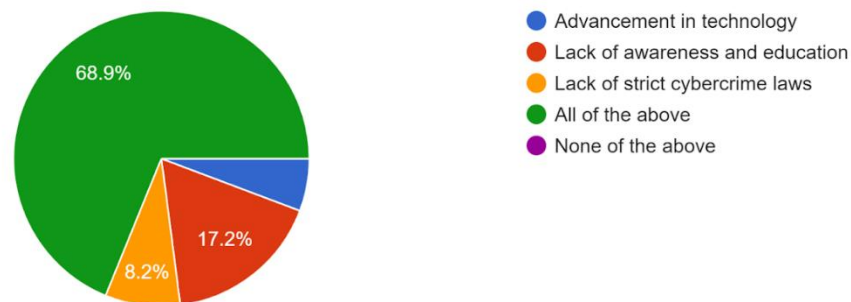


- 67.2% of respondents believe that there is no enough public awareness about the risks of cyber crime.
- 18.9% of respondents are not sure about it.
- 13.9 % of respondents believe that there is enough public awareness about the risk of cyber crime.

19. Which of the following factors do you think contribute to the rise of cyber crime?

Which of the following factors do you think contribute to the rise of cyber crime?

122 responses

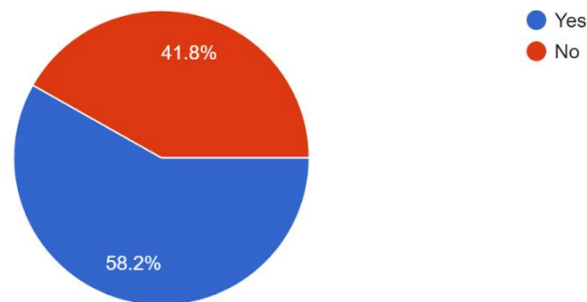


- 68.9% of respondents believe all the factors contribute to the rise of cyber crime.

20. Are you aware of any cyber crime laws implemented in your country?

Are you aware of any cyber crime laws implemented in your country?

122 responses



- 58.2% of respondents are aware of cyber crime laws implemented in their country.
- 41.8% of respondents are not aware of cyber crime laws implemented in their country.

CONCLUSION OF THE ANALYSIS

- The objective of this analysis was to explore relationships between demographic factors (age and gender) and experiences with cybercrime, including cyber bullying and the reporting of cyber crime incidents.
- The majority of respondents were between the ages of 20-25 (57%) and the gender distribution was nearly even, with 52% female and 48% male. About 21% of respondents reported experiencing cyber bullying, while only 19% reported having reported cyber crime incidents.

- Younger individuals (20-25) reported the most cyber bullying incidents in absolute numbers, but individuals above 30 showed a higher relative rate of experiencing cyber bullying. Males reported slightly more cyber bullying incidents than females. Reporting of cyber crime was generally low, with younger individuals (20-25) slightly more likely to report incidents.

SCOPE AND LIMITATIONS

Scope:

1. Focus on Victim-Centric Approach: This research aims to provide insights into the experiences of cybercrime victims in India, emphasizing their perspectives on legal issues and the challenges they face. By exploring demographic factors such as age and gender, the study seeks to understand how these variables affect individuals' encounters with cybercrime.
2. Broad Range of Cybercrime Types: The research encompasses various forms of cybercrime, including but not limited to cyberbullying, identity theft, phishing, and online harassment. This wide lens allows for a comprehensive understanding of the impact of cybercrime on different demographic groups.
3. Quantitative Analysis: Utilizing quantitative methods, including surveys and statistical analysis, the study aims to establish relationships between demographic factors and experiences with cybercrime. This will provide empirical evidence to support or refute the research hypothesis.
4. Implications for Policy and Legal Reform: The findings will offer recommendations for improving legal frameworks and victim support services in India, thereby contributing to the development of more effective policies and interventions aimed at safeguarding potential victims of cybercrime.

Limitations:

1. Sample Size and Diversity: The research may be limited by the size and diversity of the sample population. A smaller or non-representative sample could affect the generalizability of the findings to the wider population.
2. Self-Reported Data: The reliance on self-reported data from surveys may introduce bias, as individuals may underreport or overreport their experiences with cybercrime due to fear of stigma or a lack of awareness about certain incidents.
3. Focus on Demographic Factors: While the study concentrates on age and gender, other relevant factors such as socioeconomic status, education level, and geographic location might also influence experiences with cybercrime but may not be adequately addressed.
4. Dynamic Nature of Cybercrime: The constantly evolving landscape of cybercrime may limit the relevance of the findings over time. New forms of cybercrime and changing victim experiences may necessitate ongoing research beyond the scope of this study.

5. Cultural Context: The study's findings may be influenced by the cultural context of India, which may not be applicable to other regions or countries with different social norms and legal frameworks regarding cybercrime.

RECOMMENDATIONS

(A) Upgraded Casualty Bolster Services:

Establish devoted bolster frameworks for cybercrime casualties that incorporate mental counselling, lawful help, and emergency intercession administrations. These assets ought to be effectively available and custom-made to address the particular needs of diverse casualty bunches, counting minors and marginalized communities.

(B) Public Mindfulness Campaigns:

Implement comprehensive open mindfulness campaigns to teach people around the dangers of cybercrime and the accessible assets for casualties. These campaigns ought to center on preventive measures, announcing components, and the significance of cybersecurity practices.

(C) Strengthening Announcing Mechanisms:

Develop streamlined and secret detailing instruments for casualties of cybercrime. This seem incorporate a centralized online stage where casualties can report occurrences, look for help, and track the advance of their cases. Guaranteeing secrecy and assurance for casualties amid the announcing prepare is crucial.

(D) Victim-Centric Preparing for Law Enforcement:

Provide specialized preparing for law requirement organizations on taking care of cybercrime cases with a center on the needs and rights of casualties. Preparing ought to incorporate affectability preparing, understanding the mental impacts of cybercrime, and successful communication strategies.

(E) Legal System Enhancements:

Advocate for the consolidation of casualty rights inside existing legitimate systems related to cybercrime. This incorporates guaranteeing that casualties have the right to take part in lawful procedures, get opportune overhauls almost their cases, and get to compensation for harms incurred.

(F) Research on Casualty Experiences:

Conduct in-depth investigate thinks about to investigate the encounters of cybercrime casualties in India. Gathering subjective information on their challenges, needs, and results can offer assistance educate arrangements and hones that superior bolster casualties in the repercussions of cyber incidents.

(G) Collaboration with NGOs and Community Organizations:

Foster associations with non-governmental organizations and community bunches that specialize in casualty back and promotion. Collaborating with these organizations can upgrade outreach endeavors and guarantee that casualties get all encompassing support.

(H) Focus on Recovery and Reintegration:

Develop recovery programs that help casualties in revamping their lives after cybercrime episodes. This seem incorporate professional preparing, counseling, and community engagement activities pointed at lessening disgrace and advancing reintegration.

(I) Promoting Cyber Cleanliness Education:

Integrate cyber cleanliness instruction into school curriculums to engage youthful individuals with information around online security, computerized impressions, and mindful web utilize. This proactive approach can offer assistance decrease the number of future victims.

(J) Monitoring and Evaluation:

Establish instruments for continuous observing and assessment of casualty back administrations and approaches related to cybercrime. Standard evaluations can offer assistance distinguish holes, degree viability, and illuminate future enhancements in victim-centric approaches.

CONCLUSION

Cybercrime is one of the most significant problems for countries around the world today. This includes unauthorised access to information and violates security such as privacy, passwords, etc. Anyone who has Internet use. Cyber theft is a part of the cybercrime, which means robbery performed via computer or the Internet. With an increase in the number of cyber security fraud and crimes, the government is developing advanced rules that will safeguard the interests of people and protect people from any negative events happening online.
