# INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 6 OF 2025

INSTITUTE OF LEGAL EDUCATION

# INDIAN JOURNAL OF LEGAL REVIEW

**APIS – 3920 – 0001 | ISSN - 2583-2344**

**(Open Access Journal)**

**Journal's Home Page – https://ijlr.iledu.in/**

**Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/**

**Volume 5 and Issue 6 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-6-of-2025/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in


INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# AN ANALYTICAL STUDY ON THE IMPACT OF CYBERCRIME CHELLENGES ON INDIVIDUALS

**AUTHOR -** R. RAJESWARI* & DR. MARUTHAVIJAYAN S (M.A., B. L., M.B.A., (PH.D.,)**

* STUDENT AT SCHOOL OF EXCELLENCE IN LAW, THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY. EMAIL: RAJIRAJURAJU4477@GMAIL.COM

** ASSISTANT PROFESSOR AT THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY. EMAIL: MARUDHU.LAWYER@GMAIL.COM

**BEST CITATION** - R. RAJESWARI & DR. MARUTHAVIJAYAN S, AN ANALYTICAL STUDY ON THE IMPACT OF CYBERCRIME CHELLENGES ON INDIVIDUALS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (6) OF 2025, PG. 773-786, APIS – 3920 – 0001 & ISSN - 2583-2344

**ABSTRACT**

Cybercrime is emerging as a serious threat. World wide governments, police departments and intelligence units have started to react. Usage of internet has become a daily routine for majority of people for day-to-day transactions. The number of internet users has grown tremendously and so does cyber-crimes. Cyber-crime is the crime that is done using computer and network. Number of crimes is increasing day by day, and these cybercrimes can impact on individual, an organisation, or even a whole nation. The research study aims to spread awareness about cybercrimes by offering a detailed analysis of awareness, impact, and challenges to anyone vulnerable to cybercrime. This paper is an attempt to provide a glimpse on cybercrimes in India. The purpose of this research is to make awareness regarding cyber-crimes which are happening in today's world and also to create awareness of increased cyber security. The methodology adopted to study and analyse the impact and challenges caused due to cybercrimes is qualitative research. On a concluding note, the study will present suggestions to overcome the challenges and talk about the research's future scope.

**Keywords:** Cybercrimes; Government; Departments; Intelligence; Tremendously; Methodology.

## INTRODUCTION

In the modern era, technology has transformed the way we live, work, and interact. With the proliferation of digital systems, cybercrimes have emerged as a significant challenge. Cybercrimes are illegal activities that occur in the digital space, exploiting vulnerabilities in computer networks, software, and devices. These offences encompass a wide range of actions that target individuals, organisations, and even nations. Cyber criminals often operate anonymously, making it difficult to trace their origins. Different types of cybercrimes have evolved with the increasing dependency on the internet. There was a dearth of understanding about the crimes that might be perpetrated over the internet a few years ago but today in terms of cybercrime, India is not far behind the other countries, where the rate of occurrence of cybercrime is also on the rise.

Cybercrimes is defined as illegal behaviour involving a computer, a computer network, or a networked device. Most, but not all, cybercrime is conducted by profit-driven cybercriminals or hackers. Some cybercrimes target computer or devices directly in order to harm or disable them, while others target computers or networks in order to disseminate malware, unlawful information, pictures, or other things. Some cybercrime targets computers in order to infect them with a computer virus, which

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

subsequently spreads to other computers and, in some cases, whole networks.

Cybercrime is broad term that is used to define criminal activity in which computers or networks as a tool, a target, or a place of criminal activity and include everything from electronic wracking to denial of service attacks. It is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and or distribution of viruses, spam and so on. It also covers that traditional crimes in which computers or networks are used to enable the illicit activity. Cyber crime is increasing day by day, nowadays it has become a new fashion to earn money by fraud calls or to take revenge through hacking other accounts.

TYPES OF CYBERCRIMES

Cybercrime ranges variety of activities. Cybercrimes can be divided into three major categories:

A. **Cybercrimes against persons** like harassment occur in cyberspace or through the use of cyber space. Harassment can be sexual, racial, religious, or other.

B. **Cybercrimes against property** like computer wreckage (destruction of other's property), transmission of harmful programs, unauthorised trespassing, unauthorised possession of computer information.

C. **Cybercrimes against government** like Cyber terrorism.

**A. Crimes against persons are:**

- Cyber-stalking: It means to create physical threat that creates fear to use the computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- Dissemination of obscene material: It includes indecent exposure/pornography (basically child pornography), hosting of website containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- Defamation: It is an act of imputing any person to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- Hacking: It means unauthorised control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- Cracking: It means that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- E-mail spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates
- SMS Spoofing: It is a blocking through spam which means the unwanted messages, wrongdoer steals mobile phone number of any person and sending SMS from the phone number of the victim.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

- Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account malafidely.
- Cheating and Fraud: It means the person who is doing the act of cyber crime ie. Stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- Child pornography
- Assault by threat

**B. Crimes against property:**

- Intellectual property crimes
- Cyber squatting
- Cyber vandalism
- Hacking computer system
- Transmitting virus
- Cyber trespass
- Internet time thefts

**C. Cybercrimes against government:**

- Cyber terrorism
- Cyber warfare
- Distribution of pirated software
- Possession of unauthorised information

ORIGIN OF CYBERCRIME

At the beginning of 1960s, criminal regularly committed crimes via telephone lines. The perpetrators were called phreakers. Actually, there was no real cybercrime until the 1980s. one person had another persons computer to find, copy or manipulate personal data and information. The first person to be found guilty of cybercrime was Lan Murphy, also known as Captain Zap, and that happened in the year 1981. He had hacked the American telephone company to manipulate its internal clock, so that users could still make free calls at peak times.

CYBER LAWS

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act,2000 was enacted with prime objective to create an enabling environment for commercial use of IT. The IT Act specifies the acts which have been made punishable. The Indian Penal Code,1860 has also been amended to take into its purview cybercrimes.

The various offences related to internet which have been made punishable under the IT Act,2000 and IPC 1860 are enumerated below:

**a. Cybercrimes under the IT Act:**

- Tampering with computer source documents- Sec.65
- Hacking with computer systems, Data alteration- Sec.66
- Publishing obscene information- Sec.67
- Un-authorised access to protected system- Sec. 70
- Breach of confidentiality and privacy- Sec.72
- Publishing false digital signature certificates- Sec.73

**b. Cybercrimes under IPC and special laws:**

- Sending threatening messages by email- Sec.503 IPC
- Sending defamatory messages by email- Sec.499 IPC
- Forgery of electronic records- Sec.463 IPC
- Bogus websites, cyber frauds- Sec.420 IPC
- Email spoofing- Sec.463 IPC
- Web-jacking- Sec.383 IPC

- Email Abuse- Sec.500 IPC

**c. Cybercrimes under the special Acts:**

- Online sale of drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Act

**REVIEW OF LITERATURE**

The aim of this paper is to review the literature of various related to this research. Most of the articles, journals, newspapers, books, websites, have primarily focused on the topic "**Impact and Challenges of Cybercrimes on People"**. This research shall be guided by the research conducted earlier. Many researchers have their own views and opinion upon this topic. Let's crackdown the views of different researchers:

1) Neelesh Jain, Vibhash Shrivastava (2014) through " Cybercrime changing everything- An Empirical Study" recognised that:

   There is the potential for many of us to become victims to the growing pool of criminals who skilfully navigate the Net. This paper argues that Cyber crime or e-crime presents a new form of business and Hi-tech Criminals. This paper explores an overview of Cybercrimes, the cyber-crimes perpetrators and their motivations also he discussed in detail of different cybercrimes, and unique challenges and responses issue which may be encountered during the prevention, Detection and investigation and also outlined different sections of IT Act 2000 of India also proposed new provision in IT Act 2000.

2) Raj Singh Deora, Dhaval Chudasama through "Brief Study on Cybercrimes on an Internet" said that:

   His research paper engages analysis of the cybercrimes that targets individuals on the internet and also examines the motivation of criminals that perform such attacks which include online harassment, identity theft, malware, hacking, etc. is a threat to today's internet- dependent society and is a huge growing problem. By research, it is found that people using online shopping and other platforms which provide benefits and rich environment for criminal activity to steal an identity theft of classified government information.

3) Shwetha Sankhwar, Arvind Chaturvedi through "Woman Harassment In Digital Space In India" recognised that:

   Digital space has opened doors to cyber criminals and mostly women are targeted. Women and children remain at risk. Offenders are gradually misusing cyber platforms to harass and abuse women and children. This paper throws light on Cybercrime and legislative intervention measures.

4) Mohammad Hussain in his paper "Cyber Crime and Security" said that:

   In his paper he mentioned some of the impact of cybercrime. cybercrime is that activities made by the people for destroying organisational network, stealing others valuable data and documents, etc. his paper give a detailed study regarding cybercrime, its types, modes of cybercrime and security measures.

5) V. Karamchand Gandhi through his paper "An Overview Study On Cybercrimes in Internet" said that:

   Cyber crime emerged as a serious threat. World Wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are talking shape. Indian police has initiated special cyber cells across the country and have started educating personnel. This paper is an attempt to provide a glimpse on cyber crime in India.

6) Shivani Reddy in her paper "Analytical Study on Cyber Crimes in India" recognised that:

Her paper examines on the various forms of cybercrimes, cybercrimes in India and the laws and the Role of Judiciary. It also includes cybercrimes from the aspect of International laws, and the social impact in India.

**RESEARCH GAP**

All the article and journals discussed the legal aspects of cyber crimes but comparing to these articles, they failed to reveal about how the cyber crimes will affect the mindset of people and how can we just give awareness to the people for saving themselves from these cyber frauds. This study finds out the above perceptions and also find out the impact and challenges of cyber crimes and its legal perspective and also the way which we have to take for our safety.

**STATEMENT OF PROBLEM**

Cybercrime is a problem today because technology is advancing everyday , however security measures to protect this technology and the users of the technology is not advancing as quickly. This allows for cybercrimes to occur more often. This study is conducted to know the impact and challenges of the cybercrimes on various people. How these crimes affect the mindset of people, how they will overcome from cybercrimes, from where they get the awareness about the cybercrimes, etc...

**OBJECTIVES OF THE STUDY**

- To investigate how cybercrime affects various sectors of the economy, including business, government and individuals.
- To analyse the financial losses, recovery costs, and long term economic consequences.
- To examine the technological challenges
- To analyse the social and psychological impact
- To study legal and regulatory challenges
- To assess the role of cybersecurity measures
- To examine impacts on privacy
- To study public awareness and education related to cybercrimes

**METHODOLOGY OF THE RESEARCH**

**Sources of Data**

The researcher conducted the research through primary data and secondary data.

Primary Data

Primary Data is a type of data researchers directly collect from the main sources. It has been collected by the researcher himself/herself. It is available in the raw –form. It includes the real-time data. It collected to address a current research problem. It includes personal interviews, Surveys, Experiments, schedules, focused group interviews etc.., It is otherwise called as "Fresh collection of Data".

Now I collect this below solutions through Questionnaire method. Questionnaire is the main tool for collecting primary data. It has been designed in a systematic manner covering adequate and relevant questions which covers all aspects of the study. This method we have to collect the information from the people about their opinion. This questionnaire was made by using the Google-form (G-form). So this method was very useful for my research. Using these types only I had to collect the opinion from the people. People gave different aspects of opinion through this survey.

This is a non-doctrinal research, with the primary data being collected through electronic survey forms generated by Google forms and distributed to the respondents via the Internet.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 6 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Secondary Data:

Secondary data refers to a data that is collected by someone other than the primary user. It is available in the refined form. It was already existing data produced by the researchers. Referring the secondary data is very quick and easy manner. Data collection tools include Journals, articles, websites, government publications, published documents, reports and records.

Structure of Questionnaire:

For the data collection, I made my questionnaire very simple and easy questions related to my topic. This questionnaire includes Multiple Choice Questions (MCQs), Scalar type questions, open and close ended questions. I used this questionnaire and collected the data.

Sample Size

A sample size of 40 respondent both male and female from the states of Tamil Nadu and Kerala.

**LIMITATIONS OF THE STUDY**

The number of samples collected for carrying out this research was limited to a certain number of 41 respondents. And hence the data collected from small set of population. The researcher collected data from both Tamil Nadu and Kerala states. Further the study was conducted purely through online mode, which leads to lack of personal contact with the respondent. It may be assumed as accurate. So, when the questionnaire was shared to the respondents for study, some were unaware of these cybercrimes. And many of them refused to give the response. Findings of the study are based on the assumption that the respondents have given correct information.

**DATA ANALYSIS AND DISCUSSIONS**

TABLE 1: SOCIO ECONOMIC VARIABLE OF THE RESPONDENTS

| S.NO. | VARIABLES | | NO. OF RESPONDENTS | PERCENTAGE (%) |
|---|---|---|---|---|
| 1. | AGE | Below 20 | 32 | 78% |
| | | 21 – 40 | 9 | 22% |
| | | Above 40 | - | - |
| | | Total | 41 | 100% |
| 2. | GENDER | Male | 7 | 17% |
| | | Female | 34 | 83% |
| | | Total | 41 | 100% |
| 3. | EDUCATIONAL QUALIFICATION | High school | 1 | 2% |
| | | Higher secondary | 4 | 10% |
| | | College | 32 | 78% |
| | | Others | 4 | 10% |
| | | Total | 41 | 100% |

Source: Primary Data

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 6 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

INTERPRETATION:

On observing, Table 1 reveals the following:

The age of the respondents is classified as below 20, from 21 to 40 and above 40. The total number of respondents are 41. 32 of them included in below 20 which means below 20 contains 78% of total percentage, 9 of them included in from 21 to 40 ie, it contains 22% of total percentage, and there is no respondent with the age group of above 40. The gender wise classification of respondents is classified as male and female. 7 of them are male that means 17% of the total percentage are male and 34 of the respondents are female ie, 83% of the total percentage are females. The educational qualification of respondents is classified as high school, higher secondary, college and others. 1(2%) of them are high school, 4(10%) of them are higher secondary, 32(78%) of them persuing college and 4(10%) of them working in various fields.

TABLE 2: AVAILABILITY AND OTHERS FACTORS RELATED TO CYBERCRIMES

| S.NO. | VARIABLES | | RESPONDENTS | PERCENTAGE (%) |
|---|---|---|---|---|
| 1. | Type of device which the respondent have to access the internet | Smart phone | 40 | 98% |
| | | Laptop | 1 | 2% |
| | | Computer | - | - |
| | | Others | - | - |
| | | Total | 41 | 100% |
| 2. | How many hours per day the respondent is online | Occasionally | 9 | 22% |
| | | Sometimes | 19 | 46% |
| | | Always | 13 | 32% |
| | | Never | - | - |
| | | Total | 41 | 100% |
| 3. | Favourite social media platform of the respondent | Watsapp | 10 | 24% |
| | | Instagram | 26 | 64% |
| | | Facebook | 2 | 5% |
| | | Twitter | - | - |
| | | Others | 3 | 7% |
| | | Total | 41 | 100% |

Source: Primary Data

INTERPRETATION:

According to the table mentioned above, 40(98%) of the total respondents are using internet through their smart phones and only 1 of them ie, 2% of the total percentage using laptop for accessing internet. 22% of the respondents are online occasionally and 46% of them are using internet sometimes but 13 of the total respondent which means the 32% of them are always online. 24% of the

respondents are mostly using watsapp and 64% of them are using Instagram, 5% of the respondents are using Facebook and 7% of the total respondents using social platforms like You tube, telegram, etc.

TABLE 3: GUIDING QUESTIONS

| VARIABLE | YES | | NO | | MAYBE | | INDIFFERENT TO THE QUESTION | | TOTAL | |
|---|---|---|---|---|---|---|---|---|---|---|
| | No. of res | % of res | No. of res | % of res | No. of res | % of res | No. of res | % of res | No. of res | % of res |
| Are you an internet user | 41 | 100% | - | - | - | - | - | - | 41 | 100% |
| Has anyone tried to scam you in the past years | 7 | 17% | 19 | 46% | 15 | 37% | - | - | 41 | 100% |
| Have you ever heard of cybercrime or cyber bullying | 33 | 81% | 7 | 17% | 1 | 2% | - | - | 41 | 100% |
| Have you found someone using your personal data | 3 | 7% | 32 | 78% | 6 | 15% | - | - | 41 | 100% |
| Did you report | 10 | 24% | 24 | 59% | 7 | 17% | - | - | 41 | 100% |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| it to the admin website | | | | | | | | | | |
| Have you ever heard of someone being a victim of cybercrime | 32 | 78% | 9 | 22% | - | - | - | - | 41 | 100% |
| Have you seen anything on the news about people being harassed online | 32 | 78% | 4 | 10% | 5 | 12% | - | - | 41 | 100% |
| Are you satisfied with the way your complaint was handled | 11 | 28% | 12 | 30% | 13 | 32% | 4 | 10% | 41 | 100% |

Source: Primary Data

INTERPRETATION:

According to the table mentioned above, All of the respondents are the users of internet. 7 of the respondents experienced the cybercrimes, 19 of them didn't experience it and 15 of the didn't know whether they are the victim or not. 33 of the respondents are heard about cybercrimes, 7 of them not

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

heard about it and 1 of them is confused with it. 3 of the respondent is aware that someone is using their personal details, 32 of them assuring about their privacy and no one is using their personal details except them and 6 of them is confused that they didn't know whether their personal data is safe or not. 24 of the total respondents didn't report to the admin website when they felt any issues with their internet, 10 of them are reported it and 7 of them didn't know where to report. 32 of the respondents are experienced cybercrimes with their friends or relatives and 9 of them didn't have any experience. 32 of them seen these crimes in news and 4 of them didn't see it and 5 of them don't know anything about it. 11 among the 41 respondents are satisfied with the way their complaint was handled, 12 of them not satisfied with it and 13 of them didn't know about it and 4 responds as it is indifferent to the question.

TABLE 4: HOW SATISFIED ARE THE RESPONDENTS WITH EACH OF THE FOLLOWING

| VARIABLE | STRONGLY AGREE | | AGREE | | NEUTRAL | | DISAGREE | | STRONGLY DISAGREE | | TOTAL | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No. of res | % of res | No. of res | % of res | No. of res | % of res | No. of res | % of res | No. of res | % of res | No. of res | % of res |
| Sharing password with friends and family | - | - | 3 | 7% | 2 | 5% | 1 | 2% | 35 | 86% | 41 | 100% |
| Using same password for multiple websites | - | - | 1 | 2% | 2 | 5% | 8 | 20% | 30 | 73% | 41 | 100% |
| Using online storage systems to exchange and keep personal or sensitive information | 3 | 7% | 33 | 81% | 2 | 5% | 1 | 2% | 2 | 5% | 41 | 100% |
| Using free to access public | 5 | 12% | 25 | 62% | 7 | 17% | 3 | 7% | 1 | 2% | 41 | 100% |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| wifi | | | | | | | | | | | | |
| Downloading free antivirus software from an unknown source | - | - | - | - | - | - | 25 | 61% | 16 | 39% | 41 | 100% |
| Downloading digital media from unlicensed sources | 10 | 24% | 5 | 12% | 5 | 12% | 10 | 24% | 11 | 28% | 41 | 100% |
| Accepting friends request on social media because you recognise their photo | 30 | 74% | 5 | 12% | 4 | 10% | 1 | 2% | 1 | 2% | 41 | 100% |
| Sending personal information to strangers over internet | 41 | 100% | - | - | - | - | - | - | - | - | 41 | 100% |
| Clicking on links contained in unsolicited emails from an unknow | 35 | 85% | 4 | 10% | 2 | 5% | - | - | - | - | 41 | 100% |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| n source | | | | | | | | | | | | |

Source: Primary Data

INTERPRETATION:

Many of the respondents are strongly disagree with sharing passwords with friends and family. And others disagree on it. Many of the disagree with using same password for multiple websites. Many of the respondents using online storage systems to exchange and keep personal information. Some of them using free access to public wifi and others are not. No one of the respondents are downloading free antivirus software from an unknown source. Many of the respondents are downloading digital medias from unlicensed sources. Most of them are accepting friend request on social medias by recognising their photos. Many of them are not sending personal information to strangers over internet. But most of them clicking on links containing unsolicited data.

**FINDINGS**

- Cyber criminals are becoming more sophisticated in their tactics, making it challenging to detect and prevent attacks.
- Phishing remains a prevalent method for cybercriminals to deceive individuals and organisations
- Ransomware attacks continue to rise, targeting businesses, governments, and individuals
- Insider threats pose a significant risk, with employees or trusted individuals exploiting their access
- The Proliferation of Internet of Things devices has created new entry points for cyberattacks
- Many individuals and organisations neglect basic cybersecurity practices

**SUGGESTIONS**

- Promote cybersecurity awareness and education programs to help individuals recognize and respond to threats
- Encourage the use of strong, unique passwords and multi-factor authentication
- Maintain up-to-date software and security patches to address vulnerabilities
- Provide cybersecurity training to employees to prevent insider threats
- Develop a comprehensive incident response plan to mitigate the impact of cyberattacks
- Encrypt sensitive data to protect it from unauthorised access
- Foster collaboration between governments, businesses, and cybersecurity experts to share threat intelligence
- Implement security measures for IoT devices, such as default password changes and regular updates
- Consider cyber insurance to help cover the financial costs of a cyberattack
- Emphasize the importance of keeping software

**CONCLUSION**

In conclusion, cybercrimes have a profound impact on individuals, businesses and nations. Addressing the challenges requires a multi-faceted approach, including improved cybersecurity measures, international cooperation, legal reforms, and increased public awareness and education about cyber threats. As technology continues to advance,

staying ahead of cybercriminals remains an ongoing challenge for governments, organisations and individuals.

Cyber crime is a constantly evolving field, and it's essential for individuals and organisations to stay informed about the latest threats and security measures to protect themselves effectively. It's important to note that the legal framework for cybercrime is continually evolving to keep pace with technological advancements and emerging threats. Cybercrimes have significant psychological, financial and social consequences for individuals. Victims often endure stress, anxiety, and financial losses, while their privacy and reputation may be compromised. Victims of the cybercrimes encounter numerous challenges including reporting difficulties, legal complexities and the need for better support services.

Cybercrimes are characterized by their evolving and complex nature, making them challenging to detect and prevent. The use of encryption and anonymizing technologies further complicates investigations. The global reach of cybercrimes necessitates international cooperation, which can be hindered by legal and jurisdictional complexities. Many organizations and law enforcement agencies face resource limitations, hindering their ability to effectively combat cybercrimes. Balancing the need for cybersecurity with ethical considerations, including privacy rights, presents an ongoing challenge. The research underscores the importance of cybersecurity awareness, strong password policies, regular software updates, and other preventive measures. Adequate and up-to-date legal frameworks are crucial for prosecuting cybercriminals and protecting victims. Public-private partnerships, industry standards, and information sharing are essential elements of a comprehensive strategy to address cybercrimes effectively.

In light of these findings, it is evident that addressing cybercrimes requires a holistic approach involving governments, law enforcement agencies, organizations, and individuals. This approach should encompass legal reforms, technological advancements, and educational initiatives to enhance cybersecurity awareness and preparedness. As the digital landscape continues to evolve, research in the field of cybercrime remains critical. Ongoing efforts are needed to adapt to emerging threats, strengthen cybersecurity measures, and provide support for victims, ultimately creating a safer and more secure digital environment for all.

**REFERENCE**

1. V. Karamchand Gandhi, "An Overview Study On Cyber crimes in Internet", Journal of Information Engineering and Applications, ISSN 2224-5782(print) ISSN 2225-0506(online), Vol 2, No.1, 2012
2. Neelesh Jain, Vibhash Shrivastava, "Cybercrime changing everything – An Empirical Study", International Journal Of Computer Application, Issue 4, Volume 1 (February 2014)
3. Anupreet Kaur Mokha, "A Study On Awareness of Cybercrime And Security", Research Journal of Humanities and Social Sciences, Issue No. 4, Volume 8, 2017
4. Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra, "Cybercrime and Cyber criminals: A Comprehensive Study", International journal of computer networks and communications security, Volume 4, No.6, June 2016
5. Amit Wadhwa, Neerja Arora, "A Review on Cyber Crime: Major Threats and Solutions", IJARCS, Volume 8, No. 5, May-June, 2017
6. Pradheep M. D, "A Study on the Cyber Crimes in the Technological Era", Advances in Information Technology, Management, Social sciences and Education, December 2018

7. Showkat Ahmad Dar, Dr. Naseer Ahmad Lone, "Cyber Crimes in India", Vol- 43, No.4, October- December, 2020
8. Chandra Sekhar Biswal, Subhendu Kumar Pani, "Cyber-Crime Prevention Methodology", Chapter 14, November 2020
9. Raj Singh Deora, Dhaval Chudasama, "Brief Study Of Cybercrime on an Internet", Journal of Communication Engineering & Systems, ISSN: 2249-8613, Volume 11, Issue 1,202
10. Kamini Dashora, "Cyber Crime in the Society: Problems and Preventions", Journal of Alternative Perspectives in the Social Sciences", Vol 3, No.1, 240-259, 2011