



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Cybercrimes in India: Cases, Precautions, Reporting

Dr. Kiran G. Jayade¹, Dr. Sangita V. Warade², Dr. Nitin W. Raut³

Asst. Professor, Dr. PDKV, College of Agriculture, Nagpur, Maharashtra, India¹

Asso. Professor, Dr. PDKV, School of Agri-Business Management, Nagpur, Maharashtra, India²

Asst. Professor, Office of the Dean (Agri), Dr. PDKV, Akola, Maharashtra, India³

ABSTRACT: Cybercrime in India is increasing day by day, nowadays it has become a new fashion of people to earn money by doing fraud calls or to take revenge through hacking other accounts. Cyber Crime is a bi-product of the ever-increasing development in the areas of information and communication technology (ICT) as well as more people are using internet for different types of their activities on internet. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details then report complaints of cybercrime online by visiting the National Cyber Crime Reporting Portal of India at <https://cybercrime.gov.in/>. Highest number of cybercrimes are from Bengaluru, followed by Hyderabad and Mumbai. You can also file a complaint offline by dialling the helpline number 155260. Cybercrime data related to state wise, union territory wise and metropolitan cities/cases are given in this paper. Every person on the Internet should follow the precautionary measures to be safe from cybercrime.

KEYWORDS: Cybercrime, cybercrime cases, cybercrimes against persons, cybercrime precautions, cybercrime reporting.

I. INTRODUCTION

Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime". Cybercrime is a criminal activity in which digital devices (including servers, computers, tablets, iPads, smartphones, etc.) computers or computer networks are 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 distribution of viruses, spam and so on. It covers that traditional crimes in which computers or networks are used to enable the illicit activity. Cybercrime 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.

The term Internet can be defined as the collection of millions of computers throughout the world that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone is using the Internet for betterment of life but there is another side of the Internet that is Cybercrime. Cyber Crime is a bi-product of the ever-increasing development in the areas of information and communication technology (ICT). The attackers mainly attack the confidential data of the organizations or personal information thereof. The most targeted organizations for cybercrimes are individuals, government offices, servers on network, hospitals, financial, institutions, schools, colleges, university, reserve bank, state bank of India, all nationalized banks, private banks, military services, space research, defence, persons on target, research and development organizations and other telecommunication firms, etc.

II. MATERIALS AND METHODS

For this study of cybercrime in India, we used electronic gadgets namely desktop, laptops, smartphones to collect the data and information on cybercrime. We used websites of government of India, government of Maharashtra, websites of different organizations dealing with cybercrime. Studied many Research papers on cybercrimes on websites of Google Scholar. High speed internet facility were used namely, broadband internet, personal network, home network,

Wi-Fi, wireless networks, Fibre Optic internet services, mobile internet and other networks for downloading data and webpages from the different cybercrime related websites. Internet browser software viz. Google chrome, Internet explorer, Mozilla Firefox, Edge were used for opening the different related websites on the Internet. Search engines like Google, Google Scholar and other search engines have been used for searching the latest information and literature. Similarly, secondary statistical data of cybercrime cases in India are downloaded from NCRB website and government websites. All related data are downloaded, collected, cleaned, tabulated, stored and summarised. Summarised data is analysed by using different statistical analysis software and data analysis tools. Results of analysis on the data have been presented and concluded in this paper.

III. CLASSIFICATION OF CYBERCRIMES

3.1 Classification of Cybercrimes

Cybercrime are classified into three types:

A) **Cybercrimes against persons**

like harassment occur in cyberspace or through the use of social media, internet and email and cyberspace. Bank fraud, money laundering, phishing, bullying, harassment can be sexual, racial, religious, social media or other.

B) **Cybercrimes against property**

like computer destruction and others' digital property, transmission of harmful programs, deleting important data from servers and computers, unauthorized possession of computer information.

C) **Cybercrimes against government**

like Cyber terrorism.

Following are the examples of classification of cybercrime.

A) **Crimes against persons**

- **Phishing**

Phishing is the act of sending fraudulent e-mail that appears to be from a legitimate source, for example, a bank, a recruiter or a credit card company etc. This is done in an attempt to gain sensitive personal information, bank account details etc. from the victim.

- **CyberStalking**

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group. A cyber stalker targets the victim with threatening/abusive messages. It means to create physical threat that creates fear to use the computer technology such as internet, e-mail, phones, text messages, social media, webcam, websites or videos, etc.

- **Cyber bullying**

Cyber bullying is bullying that takes place over digital devices. Cyber bullying can occur through SMS, social media, forums or gaming apps where people can view, participate or share content. Cyber bullying includes sending, posting or sharing negative, harmful, false content about someone else. The intention is to cause embarrassment or humiliation. At times, it can also cross the line into unlawful criminal behaviour.

- **Hacking**

It means unauthorized control or access over computer system and act of hacking completely destroys the whole data as well as computer programmes. The attacker hacks or gains access to the social media account of the victim. The attacker can then harm the victim by misusing their personal information and photographs. The attacker can also post offensive content on victim's profile or defame the victim.

- **Dissemination of Obscene Material**

It includes illegal material exposure, pornography, hosting of web site or social media containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent children, females, males and tend to deprave or corrupt their mind.

- **Cracking**

It is one of the serious cybercrimes known till date. Cracking means that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

- **Cheating & Fraud**

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

- **Pornography**

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

- **Credit/Debit Card fraud**

The attacker tries to scare the victim by informing them that their credit/debit card has been blocked. The victim becomes worried and starts panicking. The attacker takes advantage of this situation and asks victim to provide sensitive personal information to re-activate the card. This information is then misused to steal money or cause harm to the victim. It means false ATM (Debit and Credit) cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account malafidely.

- **Online Banking Frauds**

Recently, all banking services are shifting online. Services like retrieving account statement, funds transfer to other accounts, requesting a cheque book, preparing demand draft, etc. can all be done online. As the services are shifting towards online platforms, cyber frauds related to banking are also increasing. We must protect our online bank accounts with strong passwords. If the password is stolen, then the money in the bank accounts will be stolen.

B) 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.

There are certain offences which affects person's properties which are as follows

- **Intellectual Property Crimes**

Intellectual property consists of intellectual rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. 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.

- **Cyber Vandalism**

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.

- **Hacking Computer System:**

Hacking attacks are those included famous twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

- **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.

- **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.

C) Cybercrimes against Government

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism**

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, crashing of computer operating systems and software, hate websites and hate e-mails, attacks on sensitive computer networks, etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

- **Cyber Warfare**

It refers to politically motivated hacking to damage and spying. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

- **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.

- **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, defence, ideological objectives.

IV. RESULTS AND DISCUSSIONS

4.1 Cybercrime cases in India during 2012-2018

The following table shows the cybercrime cases reported in India from the year 2012-2018.

Table 1: Total number of cybercrimes reported and increase % in India from 2012-2018.

Sr. No.	Year	Cybercrime cases in India	Increase in cybercrime (%) on YoY
1	2018	27248	25.01
2	2017	21796	76.96
3	2016	12317	6.25
4	2015	11592	20.47
5	2014	9622	69.01
6	2013	5693	68.58
7	2012	3377	88.55
	Total cases:	91645	

Source: ncrb.gov.in. YoY = year on year

The above table 1, clearly shows that every year number of cybercrime cases are increasing in India and total cases are 91645 from 2012 to 2018. Increase % of cybercrime is 68.58% in 2013 the, 69.01 % in 2014, 20.47 % in 2015, 6.25 % in 2016, 76.96 % in 2017, in 2018 increase is 25.01 % and number of cases are 27248.

4.2 Cybercrime cases State wise and UT wise in India during 2018-2020

The following table shows the state wise cybercrime cases reported in India from the year 2018-2020.

Table 2: Cyber Crimes in States and Union Territories of India (State & UT-wise) - 2018-2020

Sr. No.	States and UTs	Number of Cybercrime cases in 2018	Number of Cybercrime cases in 2019	Number of Cybercrime cases in 2020	Projected population-2020 (in lakhs)	Rate of Total Cybercrimes (2020) (cases in 2020/populations in lakh)	Yearly Increase in % of cybercrime (2018-2020)
1	2	3	4	5	6	7	8
1	Uttar Pradesh	6280	11416	11097	2289.3	4.8	38.35
2	Karnataka	5839	12020	10741	665	16.2	41.98
3	Maharashtra	3511	4967	5496	1236.8	4.4	28.27
4	Telangana	1205	2691	5024	375.4	13.4	158.46
5	Assam	2022	2231	3530	347.9	10.1	37.29
6	Odisha	843	1485	1931	454.7	4.2	64.53
7	Andhra Pradesh	1207	1886	1899	526	3.6	28.67

8	Bihar	374	1050	1512	1219	1.2	152.14
9	Rajasthan	1104	1762	1354	786.1	1.7	11.32
10	Gujarat	702	784	1283	691.7	1.9	41.38
11	Jharkhand	930	1095	1204	381.2	3.2	14.73
12	Tamil Nadu	295	385	782	761.7	1	82.54
13	West Bengal	335	524	712	977.2	0.7	56.27
14	Madhya Pradesh	740	602	699	837.6	0.8	-2.77
15	Haryana	418	564	656	292.1	2.2	28.47
16	Kerala	340	307	426	353.7	1.2	12.65
17	Punjab	239	243	378	301.8	1.3	29.08
18	Chhattisgarh	139	175	297	292.4	1	56.83
19	Uttarakhand	171	100	243	113.1	2.1	21.05
20	Delhi	189	115	168	203.2	0.8	-5.56
21	Meghalaya	74	89	142	32.6	4.4	45.95
22	Jammu & Kashmir	73	73	120	133.4	0.9	0.00
23	Himachal Pradesh	69	76	98	73.6	1.3	21.01
24	Manipur	29	4	79	31.4	2.5	86.21
25	Goa	29	15	40	15.5	2.6	18.97
26	Tripura	20	20	34	40.4	0.8	35.00
27	Arunachal Pradesh	7	8	30	15.2	2	164.29
28	Chandigarh and Dadra Nagar Haveli	30	23	17	12	1.4	-21.67
29	Mizoram	6	8	13	12.1	1.1	58.33
30	Puducherry	14	4	10	15.5	0.6	-14.29
31	Nagaland	2	2	8	21.8	0.4	150.00
32	A&N Islands	7	2	5	4	1.3	-14.29
33	Daman & Diu	0	3	3	10.4	0.3	0.00
34	Lakshadweep	4	4	3	0.7	4.4	-12.50
35	Ladakh	0	0	1	3	0.3	0.00
36	Sikkim	1	2	0	6.7	0	-50.00
	TOTAL ALL INDIA	27248	44735	50035	13533.9	3.7	41.81
	Total 3 years	122088					
	Average of 3 years	40673					

Source: ncrb.gov.in.

The above table 2, shows the tremendous increase in number of cybercrimes cases in India from 2018 to 2020. Total cybercrime cases are 122088 and average number of cybercrime cases are 40673 in three years from 2018-2020. Data clearly shows that there are 27248 cases in 2018, 44735 cases 64.18 % increase in 2019 and 50035 cases 11.85% increase in 2020. Largest number of cybercrime 11097 cases reported in 2020 are in Uttar Pradesh, followed by 10741 cases in Karnataka, third largest 5496 cases in Maharashtra, 5024 cases in Telangana, 3530 cases in Assam. In states of Odisha, Andhra Pradesh, Bihar, Rajasthan, Gujarat, Jharkhand number of cybercrime cases are in between 2000 to 1000 cases. In remaining states and UTs cybercrime cases are in between 1000 to 0 cases.

Out of the total reported cybercrime cases, the popular cybercrimes are - personal revenge, anger, fraud, extortion, causing disrepute, prank, cheating, sexually explicit act, publishing obscene material, forgery, fraud, bullying of women/children, ATM fraud, cyber blackmailing, online banking fraud, OTP fraud, phishing scams, identity theft scams, online harassment, cyber stalking, invasion of privacy, ransomware, tampering source documents, etc.

4.3 Cybercrime cases in Metropolitan cities in India during 2018-2020

The following table shows metropolitan city wise cybercrime cases reported in India from the year 2018-2020.

Table 3: Cyber Crimes in Metropolitan cities in India (State & UT-wise) - 2018-2020

Sr. No.	States and UT	Number of Cybercrimes cases in 2018	Number of Cybercrimes cases in 2019	Number of Cybercrimes cases in 2020	Actual Population (in Lakhs) (2011)	Rate of Total Cyber-crimes per lakh population (2020)	Yearly % Increase in cyber-crime (2018-2020)
1	2	3	4	5	6	7	8
1	Bengaluru (Karnataka)	5253	10555	8892	85	104.6	34.64
2	Hyderabad (Telangana)	428	1379	2553	77.5	32.9	248.25
3	Mumbai (Maharashtra)	1482	2527	2433	184.1	13.2	32.09
4	Lucknow (Uttar Pradesh)	962	1262	1465	29	50.5	26.14
5	Ghaziabad (Uttar Pradesh)	191	347	756	23.6	32	147.91
6	Ahmedabad (Gujarat)	212	171	421	63.5	6.6	49.29
7	Patna (Bihar)	115	202	312	20.5	15.2	85.65
8	Kanpur (Uttar Pradesh)	229	365	300	29.2	10.3	15.50
9	Nagpur (Maharashtra)	106	119	243	25	9.7	64.62
10	Pune (Maharashtra)	153	309	238	50.5	4.7	27.78
11	Surat (Gujarat)	155	228	204	45.8	4.4	15.81
12	Jaipur (Rajasthan)	415	544	192	30.7	6.2	-26.87
13	Chennai (Tamil Nadu)	73	118	186	87	2.1	77.40
14	Kolkata (West Bengal)	32	160	172	141.1	1.2	218.75
15	Delhi City	163	107	166	163.1	1	0.92
16	Kochi (Kerala)	48	43	62	21.2	2.9	14.58
17	Indore (Madhya Pradesh)	39	41	46	21.7	2.1	8.97
18	Kozhikode (Kerala)	27	15	12	20.3	0.6	-27.78
19	Coimbatore (Tamil Nadu)	15	8	4	21.5	0.2	-36.67
	TOTAL CITIES	10098	18500	18657	1140.4	16.4	42.38

Source: ncrb.gov.in.

Above table 3, shows the number of cybercrime in metropolitan cities of India from 2018-2020. Highest number of cybercrimes are from Bengaluru, followed by Hyderabad and Mumbai. These cities are the IT hub of India. India is the second largest online market in the world with over 658 million internet users in January 2022, ranked only behind China. We can see from the data that the number of victims of cybercrime is not a small figure hence, cybercrime is an issue of serious concern for Indian people using Internet and ICT. Lastly, as crime increases with population, Crime per lakh population (Crime Rate) may be a better indicator to assess increase or decrease in crime.

V. PRECAUTIONS FOR SAFETY FROM CYBERCRIME

Following are some of precautions to keep you safe from cybercrime:

- 1) Always download software or applications from known trusted sources only and most probably from software company website. Never use pirated software on your systems/devices.
- 2) Ensure all devices/accounts are protected by a strong PIN or password. Never share your PIN or password with anyone including your family members.
- 3) Observe your surroundings people observing your PIN before using an ATM. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.
- 4) Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Chrome, Edge, Firefox, Opera, etc.) after completion of online banking activity.
- 5) Do scan all e-mail attachments for viruses before opening them. Do not download e-mail attachments received in e-mails from unknown or untrusted sources.
- 6) Discuss safe internet practices and netiquettes with your friends and family regularly. Motivate them to learn more about cybercrimes and safe cyber practices.
- 7) Do not save your card or bank account details, aadhar number, PAN in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

VI. CYBER FRAUD INCIDENT REPORTING

Following are the procedure to report the fraud incident in India happened with you:

- 1) Visit the nearest cyber cell police station immediately. Every police station has cyber cell.
- 2) If you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details then report complaints cybercrime online, visit the National Cyber Crime Reporting Portal of India at <https://cybercrime.gov.in/>. In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialling the helpline number 155260.

VII. CONCLUSIONS

Cybercrime a term that covers crimes like phishing, credit/debit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and or distribution of viruses and so on. The most targeted organizations for cybercrimes are hospitals, government offices, servers on network, financial, institutions, university, banks, military, defence, persons on target, research and development organizations and other telecommunication firms, etc. Total cybercrime cases are 122088 and average number of cybercrime cases are 40673 in three years from 2018-2020. Cybercrimes are 27248 cases in 2018, 44735 cases 64.18 % increase in 2019 and 50035 cases 11.85% increase in 2020. Largest number of cybercrime reported in 2020 are 11097 cases in Uttar Pradesh, followed by 10741 cases in Karnataka, third largest 5496 cases in Maharashtra, 5024 cases in Telangana, 3530 cases in Assam. Most cybercrimes are personal revenge, anger, fraud, extortion, causing disrepute, cheating, sexually explicit act, publishing obscene material, forgery, fraud, bullying of women/children, ATM fraud, cyber blackmailing, online banking fraud, OTP fraud, phishing scams, identity theft scams, online harassment, cyber stalking, invasion of privacy, ransomware, tampering source documents, etc.



REFERENCES

- [1] Crime in India 2020 Statistics Volume I, NCRB, MHA, Govt. of India.
<https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf>. Retrieved 8-6-2022.
- [2] Crime in India 2020 Statistics Volume II, NCRB, MHA, Govt. of India.
<https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%202.pdf>. Retrieved 8-6-2022.
- [3] Cyber Security Awareness for Citizens, Maharashtra Cyber, Home Dept., Govt. of Maharashtra, Jan.2020.
- [4] Cybercrime India. <https://cybercrime.gov.in/UploadMedia/CyberSafetyEng.pdf>. Retrieved 7-6-2022.
- [5] Cybercrime India. https://cybercrime.gov.in/UploadMedia/instructions_citizenreportingcyberfrauds.pdf. Retrieved 7-6-2022.
- [6] Cybercrime India. <https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportCPRGRcomplaints-v10.pdf>. Retrieved 7-6-2022.
- [7] Cybercrime India. https://cybercrime.gov.in/Webform/Crime_OnlineSafetyTips.aspx. Retrieved 7-6-2022.
- [8] Legal Services India. <https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html> / Retrieved 25-5-2022.
- [9] Osman Goni, Cyber Crime and Its Classification. Int. J. of Electronics Engineering and Applications, Vol. 10, No.1, Jan.-March 2022, pp.1-16.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details