AN ANALYSIS OF CYBER CRIME IN INDIA: TRENDS, GOVERNMENT INITIATIVES AND PREVENTIVE MEASURES

Rachna Aggarwal[1*], Deepmala Kamboj[2]

Abstract
The paper presents an analysis of cyber crime data in India from 2017 to 2021, as well as the motives behind these crimes. The paper also discusses the initiatives taken by the Indian government to secure the cyber space and reduce the number of cybe crimes. Additionally, the paper provides preventive measures that individuals can follow to protect themselves from falling prey to cyber criminals. Despite the efforts made by the Indian government to curb cyber crimes, the paper concludes that the number of cyber crimes continues to increase each year. Therefore, joint efforts by the government and individuals are necessary to tackle this issue. The government needs to bridge the gap between policy making and its implementation, while individuals must use the cyber space cautiously and follow the guidelines issued by various government agencies.
Overall, the paper emphasizes the need for increased awareness and collaboration among all stakeholders to ensure the safety and security of the digital world in India.

Keywords: Cyber crime**,** Trend analysis, Government initiatives, Preventive measures

[1*] Associate Professor, Department of Mathematics, Mukand Lal National College, Yamuna Nagar, Haryana, India, Mobile No. 9466039049, E-mail id: raggarwal.math@mlncollegeynr.ac.in
[2]Associate Professor, Department of Mathematics, Mukand Lal National College, Yamuna Nagar, Haryana, India, E-mail id: dmala.math@mlncollegeynr.ac.in

***Corresponding Author**: Rachna Aggarwal
*****Associate Professor, Department of Mathematics, Mukand Lal National College, Yamuna Nagar, Haryana, India, Mobile No. 9466039049, E-mail id: raggarwal.math@mlncollegeynr.ac.in

DOI: - 10.31838/ecb/2023.12.si5.0131

Introduction

Computers, the internet, and various mobile technologies have altogether transformed our ways of living. The proliferation of digital technology, and the confluence of computing and communication devices has rejigged how we engage and view the world around us. Digital environment has taken the place of physical environment for shopping, entertainment, communication, banking and sharing information (Holt & Bossler, 2016). While overwhelmingly positive, these developments are like double-edged sword. Certainly each development also creates a place to be exploited for criminal purposes, thus upholding the axiom that crime follows opportunity. Abuse of photos shared on internet by child pornographers, online banking fraud, ATM Fraud, stalking and harassment by means of email and SMS, copyright infringement due to ease of sharing digital media are some examples how our growing reliance on computers and digital networks makes the technology itself a alluring target; either for stealing information or as a means of instigating disruption and damage (Clough, 2010). These crimes in which the offender uses special knowledge of cyberspace are referred to as cyber crimes (Furnell, 2002; Wall, 2001). In general, cyber crime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime". All over the world number of cyber crimes are rising exponentially with time causing huge financial and personal losses. In India itself, according to data released by National Crime Records Bureau (NCRB) in its reports, number of reported cyber crimes jumped from 21796 in 2017 to 52974 in 2021- a rise of 143 percent in just five years.

The objective of this study is to analyse the cyber crime data in India from 2017 to 2021, understand the motives behind these crimes, and present the initiatives taken by the government to keep these crimes in check. Additionally, preventive measures that individuals can take to protect themselves from cybercriminals will be discussed.

2. Data Analysis and discussion

The reported cyber crimes in India have been grouped into three categories namely, IT Act Cases, IPC (involving Computer as Medium/Target) Cases and Special Acts & Local Laws (SLL) (involving Computer as Medium/Target) Cases.

Number of reported cyber crime cases under each of these categories and motives behind the cyber crimes for a period of five years from 2017 to 2021 as given in NCRB Crime in India Reports (2017-2021) has been presented in Tables 1-4.

The variation of number of cyber crime cases across a period of five years i.e. from 2017 to 2021 for different type of offences and motives have been shown in figures 1-4.

2.1 IT Act Cases

The analysis of cyber crime trends under the IT Act from 2017 to 2021 indicates that computer-related offences, including identity theft, cheating by personation, ransomware, violation of privacy, and dishonesty receiving stolen computer resource or communication device, constitute 23%-27% of all cybercrimes under the Act, as shown in Figure 1. Additionally, the cases of publication/transmission of obscene/sexually explicit acts in electronic form are also increasing with time.

Further insights can be gleaned from Table 1, which shows a significant 66% increase in cyber crimes under the IT Act in 2019 compared to 2018. This rise can be attributed to the increasing number of individuals in India with access to internet, which increased from 462.1 million in 2018 to 560 million in 2019.

Table 1. Cyber Crimes - IT Act Cases

Sr. No.	Type of Offence	No. of Cases				
		2017	**2018**	**2019**	**2020**	**2021**
1	Tampering Computer Source Document	233	257	173	338	55
2	Computer Related Offences	10108	14141	23612	21926	19915
3	Cyber Terrorism	13	21	12	26	15
4	Publication/ transmission of obscene/sexually explicit act in electronic form	1768	3076	4187	6308	6598
5	Interception or Monitoring or decryption of Information	4	6	9	7	2
6	Un-authorized access/attempt to access to protected computer system	2	0	2	2	3
7	Abetment to Commit Offences	0	1	0	1	7
8	Attempt to Commit Offences	4	13	14	18	5
9	Other Sections of IT Act	1503	980	2720	1017	827
	Total Cyber Crimes under IT Act	**13635**	**18495**	**30729**	**29643**	**27427**

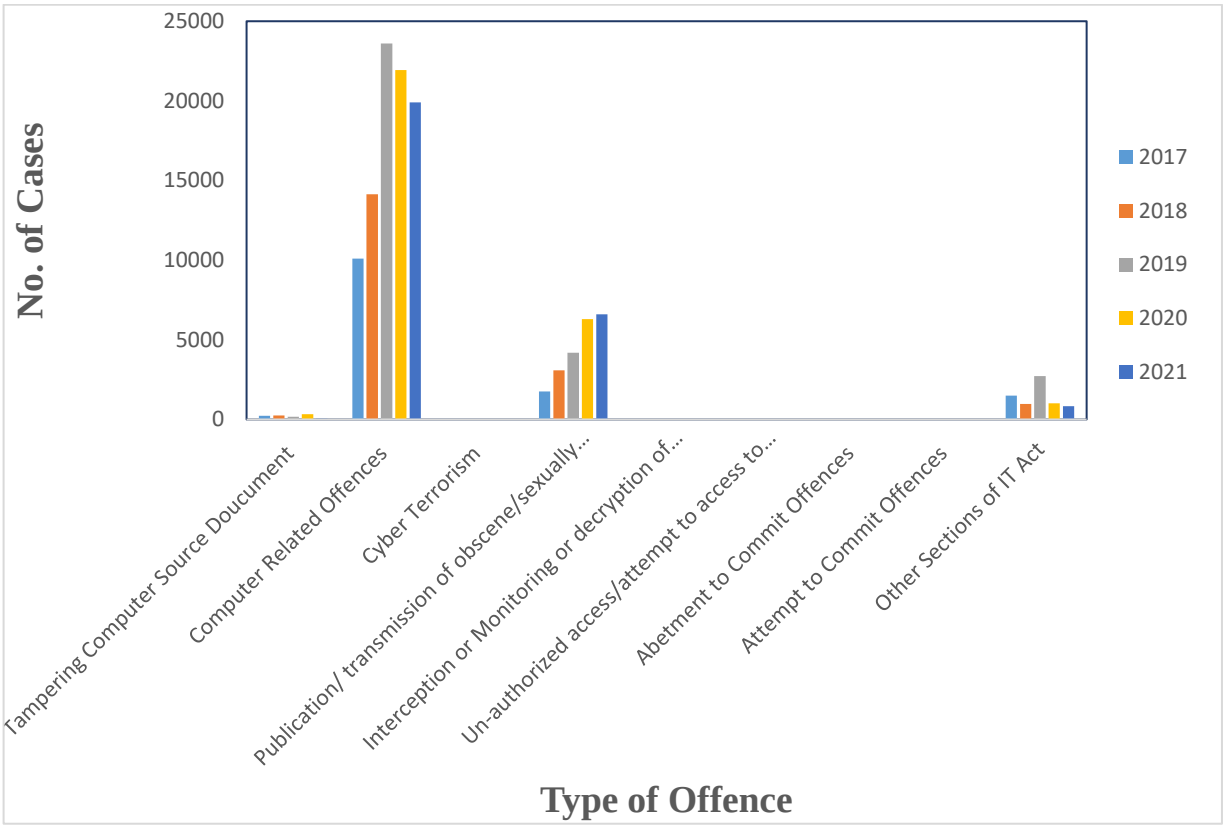

Fig 1. Cyber Crimes under IT Act

2.2 IPC (Involving Communication Devices as Medium/Target) Cases

The graph in Fig. 2 reveals a troubling trend in fraud cases related to credit/debit cards, ATMs, online banking, and OTPs in India. Over the five-year period from 2017 to 2021, the number of such cases grew exponentially, likely due to the significant increase in digital transactions during this time. As reported by Press Information Bureau, Delhi on 08-02-2023, digital transactions in India rose from 20.71 billion to 55.54 billion during this period. The more transactions that occur, the greater the chances of individuals being duped by cybercriminals.

In addition to these trends, Table 2 highlights a sharp rise in cyber crimes under IPC in 2019, which increased by 58.8% compared to 2018. This suggests that cyber crime is becoming an increasingly prevalent issue in India.

It is important to note that the fraud cases category encompasses a range of fraudulent activities, such as online banking fraud, credit/debit card fraud, ATM fraud, OTP frauds and other forms of financial fraud. Despite efforts by law enforcement agencies and financial institutions to prevent these crimes, cybercriminals continue to find ways to exploit vulnerabilities in digital systems and networks.

Table 2. Cyber Crimes - IPC (Involving Communication Devices as Medium/Target)

Sr. No.	Type of Offence	No. of Cases				
		2017	2018	2019	2020	2021
1	Abetment of Suicide (Online)	0	7	8	10	10
2	Cyber Stalking/Bullying of Women/Children	542	739	777	872	1176
3	Data theft	307	106	285	98	170
4	Fraud	3466	3353	6233	10395	14007
5	Cheating`	1896	2051	3393	4480	6343
6	Forgery	99	260	512	582	198
7	Defamation/Morphing	12	18	19	51	31
8	Fake Profile	86	78	87	149	123
9	Counterfeiting	1	2	5	9	2
10	Cyber Blackmailing/Threatening	311	223	372	303	689
11	Fake News on Social Media	170	97	190	578	179
12	Other Offences (r/w IT Act)	1086	1713	1849	2674	2456
	Total Cyber Crimes under IPC	**7976**	**8647**	**13730**	**20201**	**25384**

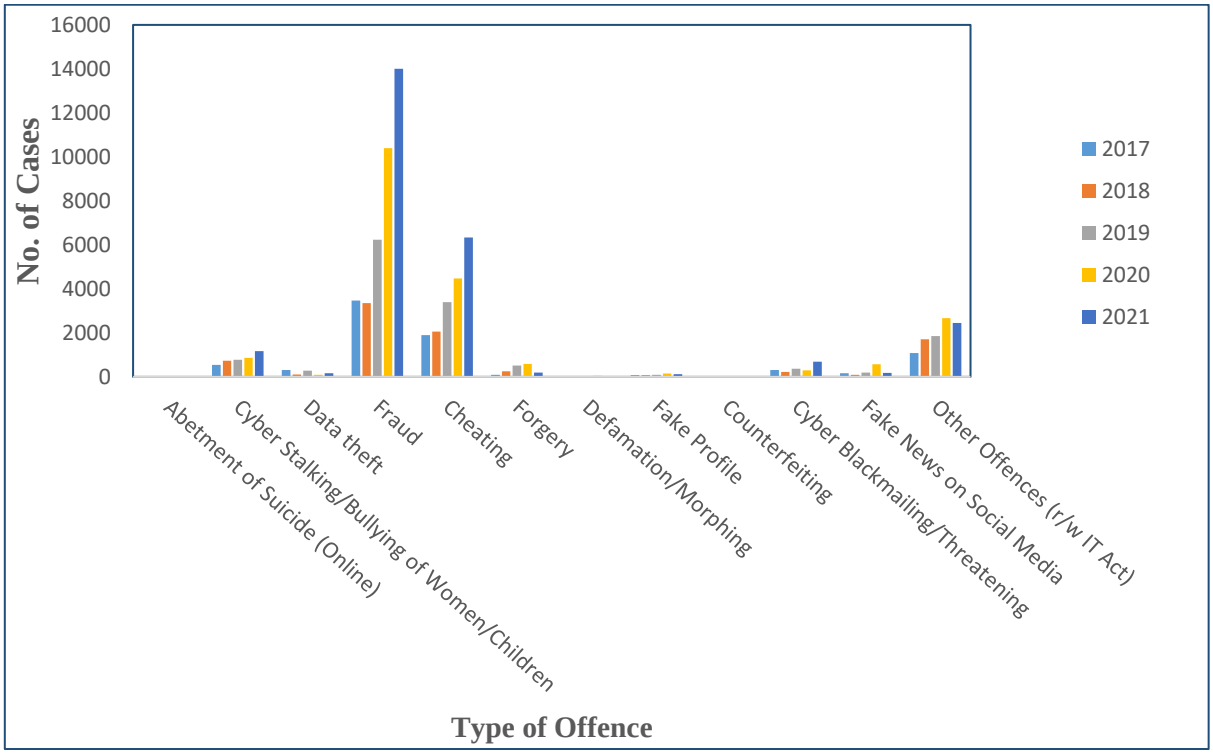

Fig 2. Cyber Crimes under IPC

2.3 SLL Cases

Table 3 indicates that cyber crimes under the Special and Local Laws (SLL) category are significantly lower in number compared to the other two categories. In the years 2017, 2018, 2019, 2020, and 2021, they accounted for only 0.85%, 0.39%, 0.20%, 0.38%, and 0.31%, respectively, of the total reported cyber crimes. On the other hand, Fig. 3 suggests that there is no discernible trend in SLL cases.

Table 3. Cyber Crimes - Offences under Special Acts & Local Laws (SLL) (Involving Communication Devices as Medium/ Target)

Sr. No.	Type of Offence	Total No. of Cases				
		2017	2018	2019	2020	2021
1	Gambling Act (Online Gambling)	45	20	22	63	27
2	Lotteries Act (Online Lotteries)	11	2	9	26	4
3	Copy Right Act, 1957	89	62	34	49	32
4	Trade Marks Act, 1999	11	0	0	5	1
5	Other SLL Crimes	29	22	22	48	99
	Total Cyber Crimes under SLL	**185**	**106**	**87**	**191**	**163**

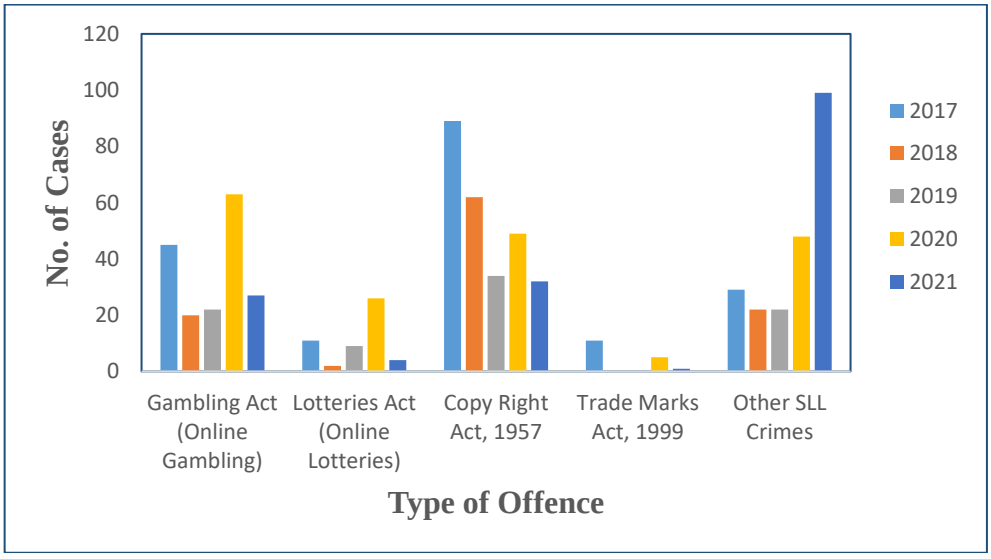

Fig 3. Cyber Crimes under SLL

2.4 Motives behind Cyber Crimes

Table 4 shows that the primary motive behind 39% to 45% of reported cybercrimes is fraud, indicating that financial gain is the most common incentive for such crimes. The next two primary motives are sexual exploitation and extortion. Fig. 4 illustrates that the number of cybercrimes with the motives of fraud, sexual exploitation, extortion, anger, and revenge has been increasing every year, while cyber crimes with other motives have been decreasing.

Table 4. Cyber Crime Motives

Sr. No.	Motive	No. of Cases				
		2017	2018	2019	2020	2021
1	Personal Revenge	628	794	1207	1470	1724
2	Anger	714	461	581	822	883
3	Fraud	12213	15051	26891	30142	32230
4	Extortion	906	1050	1842	2440	2883
5	Causing Disrepute	1002	1212	1874	1706	1715
6	Prank	321	296	1385	254	240
7	Sexual Exploitation	1460	2030	2266	3293	4555
8	Political Motives	139	218	316	356	311
9	Terrorist Activities	110	44	199	113	11
10	Inciting Hate against Country	206	218	49	165	31
11	Disrupt Public Service	55	21	28	92	40
12	Sale Purchase illegal drugs	8	6	10	21	14
13	Developing own business	156	198	181	210	177
14	Spreading Piracy	90	671	45	75	74
15	Psycho or Pervert	17	4	1	0	3
16	Steal Information	10	16	93	62	40
17	Abetment to Suicide	5	2	0	0	0
18	Others	3756	4956	7578	8814	8043
	Total Cases	**21796**	**27248**	**44546**	**50035**	**52974**

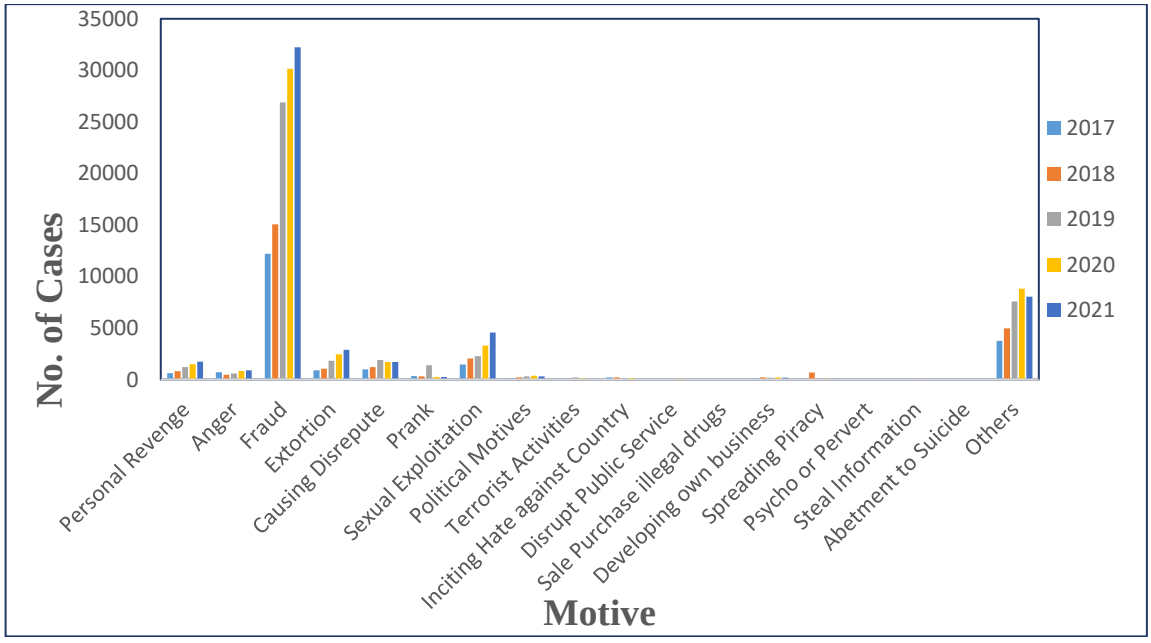

Fig 4. Motive of Cyber Crime

3. Government initiatives to prevent Cyber Crimes

Many initiatives have been taken by Indian government and several law enforcement agencies to constrain the rising cybercrimes in India. Some of the measures taken are:

- **Digital Personal Data Protection Act, 2022**

This Act was introduced to ensure the protection of user's personal data from any unauthorized use. Personal data may be processed only for a lawful purpose after obtaining one's consent. This Act also proposes to establish the Data Protection Board of India to determine non-compliance with the provisions of this Act and impose penalty under the provisions of this Act.

- **Indian Computer Emergency Response Team (CERT-In)**

CERT-In operational since 2004 is the National Nodal Agency for responding to computer security incidents as and when they occur. Its functions

include collection, analysis and dissemination of information on cyber incidents, forecast and alert of cyber security incidents, emergency measures for handling cyber security measures, issue guidelines, advisories etc. related to information security.

- **Cyber Surakshit Bharat**

This initiative was conceptualised with the mission to spread awareness about cyber-crime and build capacities of Chief Information Security Officers and frontline IT officials, across all the government departments, for ensuring adequate safety measures to combat the growing menace and for organizations to defend their digital infrastructures and become future ready in tackling cyber-attacks. The program offers training and awareness sessions, workshops, and seminars on various aspects of cybersecurity, including best practices, threat intelligence, risk management, and incident response. The initiative is supported by the Ministry of Electronics and Information Technology, Government of India, and is implemented by the Data Security Council of India (DSCI) in partnership with the National e-Governance Division and industry partners.

- **Cyber Swachhta Kendra**

Cyber Swachhta Kendra is a Botnet Cleaning and Malware Analysis Centre (BCMAC), operated by CERT-In to create a secure cyber space by detecting Botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. This centre works in close collaboration with Internet Service Providers and Product/ Antivirus companies.

- **Indian Cyber Crime Coordination Centre (I4C)**

The Ministry of Home Affairs has set up I4C to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner. Following are the main initiatives taken under I4C:

(i) The state of the art National Cyber Forensic Laboratory has been established, as a part of the I4C, at CyPAD, Dwarka, New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police.

(ii) The National Cyber Crime Reporting Portal (www.cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.

(iii) The Citizen Financial Cyber Fraud Reporting and Management System, under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters.

(iv) The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under the Indian Cyber Crime Coordination Centre (I4C), for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification.

(v) Seven Joint Cyber Coordination Teams have been constituted under I4C covering the whole country based upon cyber crime hotspots/ areas having multi-jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the LEAs of the States/UTs.

- **National Intelligence Grid (NATGRID)**

The NATGRID has been envisaged as a robust mechanism to track suspects and prevent terrorist attacks with real-time data and access to classified information like immigration, banking, individual taxpayers, air and train travels.

4. Preventive measures for individuals to avoid cyber crime

Although many initiatives have been taken by the government of India, but data released by NCRB clearly shows that there is rise in cyber crime cases every year. It clearly indicates that joint efforts by individuals and government are necessary to control cyber crimes. Following are some recommendations for avoiding the risk of victimisation by cyber offenders:

- **Maintain Good Cyber Hygiene**

(i) Keeping your devices well-organised and up to date with the latest updates and security patches can help protect your personal information and data from cyber-attacks. Updates and security patches often include critical security fixes, so it's important to keep your devices updated.

(ii) Using strong, unique passwords for all your accounts is an important step in protecting your online security.

(iii) Deleting unused apps and old accounts can reduce the risk of cyber-attacks, as hackers can use these accounts to gain access to your personal information.

(iv) Installing antivirus software that performs constant online scans can help protect your devices from cyber-attacks and notify you if there is a cyber threat or breach. Antivirus software can also detect and remove malicious software that may have infected your device.

(v) It's important to avoid downloading anything from suspicious websites, as they may contain malware or other malicious software that can infect your device. Always check the website's URL before downloading anything. A website URL beginning with "https" indicates that the website is secure.

(vi) Using a Virtual Private Network (VPN) can help protect your online activities from cybercriminals by encrypting your internet traffic. VPNs can also help protect your online privacy by hiding your IP address and location.

- **Guard Against Fraudulent Transactions (Reserve Bank of India booklet, 2022)**

(i) Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
(ii) Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
(iii) Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
(iv) Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform the authorities.
(v) Never share confidential information such as username / password / card details / CVV / OTP with anyone.
(vi) Always be careful when you are buying or selling products using online sales platforms.
(vii) Always remember that there is no need to enter PIN / password anywhere to receive money. If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.
(viii) While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.
(ix) To avoid ATM scams, always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction. Never write the PIN on your ATM card. Do NOT enter the PIN in the presence of any other / unknown person standing close to you. Do not follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs. If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.
(x) Be watchful about SIM cloning. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.
(xi) Always contact your bank/ company through official customer care number which are never in the form of mobile number.
(xii) Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.
(xiii) Do not share personal and confidential information on social media platforms.
(xiv) Avoid using public / unknown charging ports / cables.
(xv) Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.
(xvi) Never click on links sent through SMS / emails or reply to promotional SMS / emails.

- **To check publication/ transmission of obscene/sexually explicit act in electronic form**

(i) It is essential to be cautious while sharing personal and sensitive information online, especially on social media platforms. Cybercriminals can use this information for identity theft, cyberstalking, cyberbullying, and cyber sexual harassment. Therefore, it is crucial to limit the amount of personal information shared online.
(ii) Make sure that the privacy settings of your social media accounts are set to the highest level. This will help prevent your personal information and content from being shared or accessed by unauthorized persons.
(iii) It is important to report and block anything suspicious and potentially harmful in cyberspace immediately. This can help prevent further dissemination of the content and also enable authorities to take action against the cybercriminals.
(iv) Sensitizing children and their parents about cyber crimes involving children like child pornography, cyberbullying, cyber grooming, etc., can help them stay safe and handle such situations better. Parents can support their children and guide them on how to stay safe online.
(v) Organizing cyber awareness programs for children in educational institutes can also help make them aware and alert about the possible ways that can make them a victim of a cyber crime. Such programs can educate children about safe online behavior, the risks associated with social media, and how to stay safe online.
Overall, these measures can help prevent the publication/transmission of obscene/sexually explicit act in electronic form and make the digital world a safer place for everyone.

5. Conclusion

The study conducted an analysis of cybercrime data in India from 2017 to 2021 and observed that the majority of cybercrimes were related to computer-related offenses, fraud, and publication or transmission of obscene/sexually explicit acts in electronic form. The primary motives behind these crimes were fraud, sexual exploitation, extortion, anger, and revenge.

The study also found that cyber crimes in India are increasing every year, with the most significant increase of 63.5 percent observed in 2019. Despite government efforts, the trend of cyber crimes is on the rise, which calls for joint efforts of both the government and individuals.

To reduce cyber crimes in India, the study recommends that the government needs to bridge the gap between policy making and its implementation. Meanwhile, individuals should use the cyber space cautiously and follow the guidelines issued by various government agencies.

In conclusion, the study emphasizes the importance of increased awareness and collaboration among all stakeholders to ensure the safety and security of the digital world in India.

References

1. Holt T.J. & Bossler A.M. (2016). Cybercrime in Progress: Theory and prevention of technology-enabled offenses. Routledge.
2. Clough, J. (2010). Principles of Cybercrime. Cambridge University Press.
3. Furnell, S. (2002). Cybercrime: Vandalizing the Information Society. Addison-Wesley.
4. Wall, D.S. (2001). Cybercrimes and the Internet. In D.S. Wall (Ed.), *Crime and the*
5. *Internet* (pp. 1–17). Routledge.
6. National Crime Records Bureau. (2018). *Crime in India 2017, Volume II*. Government of India, Ministry of Home Affairs, National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202017%20-%20Volume%202_0_1.pdf
7. National Crime Records Bureau. (2019). *Crime in India 2018, Volume II*. Government of India, Ministry of Home Affairs, National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/Crime%20in% 20India% 202018%20-%20Volume%202_1_0.pdf
8. National Crime Records Bureau. (2020). *Crime in India 2019, Volume II*. Government of India, Ministry of Home Affairs, National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/CII%202019% 0Volume%202.pdf
9. National Crime Records Bureau. (2021). *Crime in India 2020, Volume II*. Government of India, Ministry of Home Affairs, National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/CII%202020% 0Volume%202.pdf
10. National Crime Records Bureau. (2022). *Crime in India 2021, Volume II*. Government of India, Ministry of Home Affairs, National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/CII-21/CII_2021Volume%202.pdf
11. Reserve Bank of India. (2022). *Be(A)ware: A Booklet on Modus Operandi of Financial Fraudsters*, Consumer Education and Protection Department, Reserve Bank of India, Mumbai Office. https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf