International Journal of Finance and Commerce
www.commercejournals.com
Online ISSN: 2664-715X
Received: 15-11-2025, Accepted: 10-01-2026, Published: 27-01-2026
Volume 8, Issue 1, 2026, Page No. 14-18

Rising cybercrimes in India- Negative side of proliferation of digital technologies

Ankit Raj
Research Scholar, Department of Commerce and Business Administration, Lalit Narayan Mithila University, Darbhanga, Bihar, India

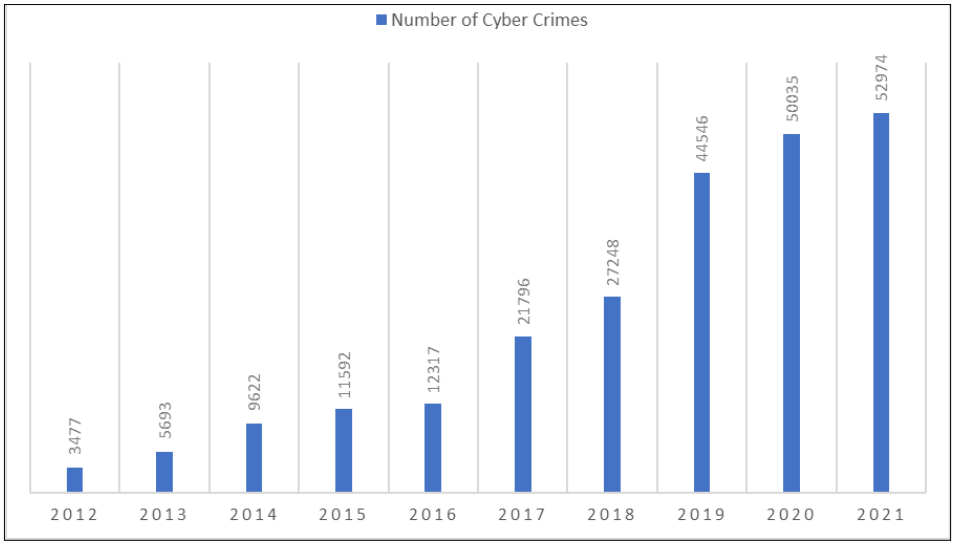
Abstract
It is a matter of pride that India has the second largest internet connection in the world. While having greater connectivity promises large-scale progress, it also leaves the citizens of our country exposed to new online vulnerabilities. Cybercrime refers to criminal activities that are carried out using the internet or other forms of digital communication technology. Cybercriminals use these technologies to commit a wide range of criminal activities, including hacking, identity theft, phishing, cyber bullying, and online scams.
The development of digital technologies has led to the growth of the Internet, social media, and other digital platforms that have become essential components of modern life. Criminals have found new ways to exploit vulnerabilities in these technologies. The rise of the internet and digital communication technologies has led to a corresponding increase in cybercrime, which has become a major concern for Governments, Businesses, Corporates and Individuals around the world. They may target individuals, businesses, or even Governments to gain access to sensitive information, financial data, or intellectual property.
The consequences of cybercrime can be severe and wide-ranging. Victims may suffer financial losses, damage to their reputation, or even physical harm, Governments and businesses may also be affected, with cyber-attacks leading to the loss of confidential information, disruption of critical services, and other serious consequences. The proliferation of digital technologies has created new opportunities for criminals to carry out their activities.

Keywords: Cybercrimes, hacking, information technology act 2000, phishing, spamming

Introduction
Cybercrime is a crime of any illegal activity committed either on or with a computer and the internet to steal personal identity, gaining unauthorised access to computer systems, sell contraband online or stalk victims online or disrupt operations with malevolent programs
Through the medium of Internet fraudsters' gain valuable sensitive information of companies, firms, individuals, banks and so forth. It can also lead to intellectual property crimes like stealing new product launch plans, new product description and marketing plans, list of potential customers, selling illegal articles, pornography/child pornography etc.
It is done using methods such as Phishing, Spoofing, Spamming, Pharming and so forth. Phishing refers to "an attack using mall programs to deceive internet users into disclosing confidential information that can be then exploited for illegal purposes".
Cybercrimes lead to financial loss, reputational loss, legal consequences, sabotage and theft of IPR. Human being is the weakest link and hence any negligence of human beings enables criminals to commit cybercrimes. Cybercrimes are now committed using mobile phones, tablets, Personal Digital Assistants (PDA) which has connectivity to internet.
Cybercrimes can cross borders in fractions of a second and impact several people in different countries at the same time. Melissa virus triggered havoc across the countries.
On March 26, 2009, Microsoft Word 97 and Microsoft Word 2000 propagated Melissa virus via e-mail attachments. Its widespread attack affected a variety of sites throughout the internet. In Melissa attack, the email attachment is a DOT Word document that contained a piece of malicious micro code. If an infected document in Word 97 or Word 2000 is opened, the embedded micro code will infect the Normal.dot template and cause any documents referencing this template to be infected with this macro virus.
Melissa virus is not the only virus that propagates itself through email attachments. Other viruses such as I Love You Virus (year 2000) and My Doom (year 2004) also propagates itself through email attachments.

Cybercrime: The Most Prevalent crime
Phishing scams can be used to trick people into providing personal or financial information, while online scams can be used to defraud people of their money. Cyberbullying is also a growing problem, with individuals using digital technologies to harass, Intimidate, or threaten others.
The rapid growth of the Internet and digital communication technologies has also made it difficult to track and prosecute cybercriminals. Many cybercriminals operate across national borders, making it difficult for law enforcement agencies to coordinate and investigate crimes. Additionally, the nature of digital communication technologies makes it easy for cybercriminals to conceal their identities and location, further complicating law enforcement efforts.
As a result, there is a growing need for greater collaboration and cooperation between Governments, law enforcement agencies, and the private sector to combat cybercrime. This includes the development of new technologies and strategies for preventing and detecting and responding to cybercrime by Governments and organisations, as well as increased investment in law enforcement and Intelligence capabilities. It also involves greater public awareness and education about the risks and dangers of cybercrime.
These can include cyber security protocols, data protection

laws, and the establishment of specialized law enforcement agencies. Preventive steps that Individuals and organizations can take to protect themselves from cyber threats. However, the constantly evolving nature of cybercrime means that these measures must continually be updated and improved to stay ahead of the latest threats.



Source: www.statista.com

Chart 1: Number of Cybercrimes Reported Across India (from 2012 to 2021)

India saw a significant jump in cybercrimes reported in 2021 from the previous year possibly due to COVID pandemic forcing most of the citizens to transact online. That year, over 52 thousand cybercrime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. A majority of these cases were registered under the Information Technology Act, 2000 with the motive to defroud, or sexually exploit victims.

Traditional white collar crime and Cybercrime

Traditional white collar crimes include Bribery, Corruption, Embezzlement or theft Forgery, Money laundering, Financial statements fraud, Identity theft, Procurement and contract fraud, Siphoning of funds and so on.

In both crimes there is no bloodshed and are perpetrated against individuals, society, organisations and the governments. The main difference lies in the modus operandi since in the case of cybercrime physical presence at the venue of the crime is not required.

In both the crimes fraud trail is left as an evidence which can be only detected by trained forensic experts. Let us understand how a computer can be a target and also used as a tool for committing cybercrime.

Computer as a Target

The computer system/ information stored on the computer are the target of the crime. Hackers broke into the system of Citibank in USA on 9th June, 2011 and accessed the data of its customers, gained access to the online banking platform and viewed customer account numbers, contact information. A There are other cybercrimes using computer as a target like virus/worm attacks, Distributed Denial of Service (DDoS), Pornography etc.

Computer as a tool

The computer system/ or Information stored on the computer system constitutes an important tool for committing the crime. Computer fraud, forgery like counterfeit currency notes, mark sheets, stamp papers, degree certificates can be done using sophisticated computers, printers and scanners, distribution of child pornography etc.

Motive and Reasons for Cybercrimes

Greed, Power hunger, Publicity, Revenge, Adventure or thrill seeking, Destructive mindset, Desire to access forbidden information have been observed as the motive and reasons for all Cybercrimes in the world.

Classification of Cybercrimes

Against Individuals: E-mail spoofing and other online frauds, Phishing, Spear Phishing, Vishing, Smishing, Spamming, Cyber defamation, Cyberstalking, Computer sabotage, Password sniffing, Pornographic offences and transmitting virus. These crimes are directed against individuals for various reosons ranging from greed to personal dispute.

Against Organisation: Hacking, Password sniffing, Denial of Service attack under section 43 of Information Technology Act, 2000, E-mall bombing, Salami Attack/Salami technique, Trojan Horse, Dato Diddling, Industrial espionage, Software privacy, Cyber terrorism by rogue actors against any organisation.

Against Society and Governments: Hacking, Forgery (printing of counterfeit currency, forging passports, sale of illegal articles, online gambling, fake Stamp papers (Telgi scam) Cube terrorism, Web jacking are directed against the society at large.

Against Property: Intellectual property, Credit card frauds, Internet time theft. Property refers also to software, computer source codes. These types of crimes are generally targeted against the society.

Accordance to the Information Technology Act, 2000, “a Cyber Crime can be defined as "an act or omission that is punishable under the Information Technology Act, 2000".

This however is not an exhaustive definition as the Bhartiya Nyaya Sanhita also covers certain cyber-crimes, such as email spoofing and cyber defamation, sending threatening emails, etc.

Types of Cyber Crime

E-mail spoofing/Phishing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. Free website are available to send fake emails. Anyone can fill any email address with the intention of deceiving the recipient of the email. When gullible receiver reads the mail/ he or she would think that the e-mail has been sent by legitimate sender based on the IP address indicating that the message has come from o trusted host. Phishing is an alternative of fishing, means to fish for information.

The term Phishing was used in 1994-95 by hackers who were stealing American Online internet accounts by scamming passwords without the knowledge of AOL users (netizens). It is also an example of social engineering techniques used to deceive netizens. This was done using www.aol.com instead of www.aol.com

Phishing is done to steal valuable personal and financial data like credit card details, passwords, PIN, social. Security numbers and bank account numbers by luring the victim to provide the account details and other personal Information unwittingly.

Denial of Services/Distributed Denial of Services

It is an attack to make a computer or network resource unavailable for the users either temporarily or permanently. DoS attackers target sites or services hosted by banks, airlines, hotel, credit card payment gateways etc. Cybercriminals prevent an internet site form functioning temporarily or even permanently.

Another Bot is a spambot, which gathers valid email addresses, so mailing lists can be created to send SPAM. Bots are particularly dangerous when they're deployed to large collections of computers, colled botnets. Once c computer is infected, the bot can lay dormant until an attacker chooses to activate them. At this point, the attacker has control of targeted computer (now called a zombie) and all the other computers in the botnet (also called a zombie army). The attacker can send a signal to have these computers distribute viruses, or send messages to a particular server in a coordinated attack called a Distributed Denial of Service attack.

It results in enormous financial and reputation loss as a result of such denial of service attack. It also leads to significant loss of time and money for the victim organisation as they have to rebuild from scratch. There have been a number of instances of DoS attacks against India.

Distributed denial-of-service (DDoS) attacks are growing significantly across the world, and India ranks second as the largest source of Hypertext Transfer Protocol or HTTP-based DDoS attack traffic in July-September this year after China. China replaced the US as the main source of HTTP DDoS attack traffic in Q3.

Hacking

It was at Massachusetts Institute of Technology the word "Hack" was used in the late 1950's. In the 1960's the term seems to have migrated from the MIT to computer enthusiasts and in time, it has become an essential port of their lexicon. The meaning of hacking at that time was "fussing with machines".

Major reasons for hacking has been identified as: Greed, publicity, revenge, adventure and destructive mindset, strong desire to access forbidden and highly confidential information. Hackers write or use ready-made computer programs to attack the target computer and get enjoyment out of destruction. They exhort money from corporates threatening them that they will publish their stolen information. Government websites are always on hacker's target and attacks on the Government websites get wide publicity.

Every act committed towards breaking into computer and/or network is hacking and Hacking with intent or knowledge is an offence under section 66 of Information Technology Act, 2000 with a Fine of Rs.2 Lakhs and imprisonment for 3 years.

Data Attacks

According to 2022 Verizon Data Breach Investigation Report (DBIR) 5,212 breaches were analysed, 23,896 security Incidents were reviewed. 82% breach involved the human element including social attacks, errors and misuse, 13% increase in Ransom ware breaches which is more than in the last 5 years combined and 62% of Incidents in the system intrusion pattern involved threat actors compromising partners. Over 50% of breaches involved use of either remote access or web applications. About 66% of breaches involved Phishing, stolen credentials and/or Ransom ware.

The four key paths to data breaches are: Credentials, Phishing, Exploiting vulnerabilities and Botnets. No organisation is safe without a way to handle them.

Data Diddling

It is one of the oldest form of computer crimes since the advent of electronic data processing. Data Diddling is changing of data either before or during entry into the computer system. Examples include forging or counterfeiting documents used for any data entry and replacing valid disks and tapes with tampered or modified disks and tapes. One of the earliest data diddling fraud was Equity Funding Corporation of America.

The NDMC Electricity Billing Fraud took place in 1996. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and payment in the bank were exclusively left to a private contractor who was a computer professional.

Masquerading

When a perpetrator pretends to be someone he is actually not by creating fake email ids, or uses someone else's user ID and password, it is called masquerading. Cybercriminals browse the Facebook profiles and identity those posting profile pictures in police uniform and download profile picture and other photos. They also download the contact names of friends. They create fake account in the same name by using the downloaded photos from original social media account. They then send friend request to contact list and asks for money later. Fraudsters want money to be transferred to them through Google Pay, Paytm, PhonePe etc

Many examples are: Scammers offering to help the account holders with bank KYC updating by asking them to

download an app and also by sharing the OTP. They also ask the victim to share the debit card details and OTP by claiming that the call is from the Bank.

Spamming
Spam is abuse of electronic message systems by sending unsolicited bulk messages indiscriminately. Spamming is difficult to control since it is difficult to hold senders accountable for their mass mailings.
Botnet Email spam- though email is seen today as an older path for attack, spam botnets are some of the largest in size. They are primarily used for sending out spam messages, often including malware, in towering numbers from each bot. The Cutwall botnet founded in 2007, con send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.

Smishing
The term is derived from SMS + PHISHING. The pretender hides the purpose and/or identity to get the personal Information/sensitive data about another individual. The criminal impersonates a legitimate entity such as an IT service/security admin, a bank, a government agency, an e-commerce site, a package delivery service, etc.

Spear Phishing
Any highly targeted e-mail attack that a scammer sends only to people within a small group. E-mail sent by the scammer appears genuine to all employees or members within the company or a Government department. Phishing scams are designed to steal information from Individuals, Spear Phishing aims to gain access to an organisation's entire computer system. E-mail message might appear to be genuine, but if the recipient responds to it, he or she might put himself or herself and the employer at huge risk.
In Spear Phishing, targets are carefully chosen, and emails are carefully crafted with the specific target in mind.

Whaling
This form of Spear Phishing targets top management C-Suites executives with the help of information obtained through Spear Phishing by installing malware for key logging or other backdoor access mechanisms. E-mail is sent in the Whaling scam showing a sense of falsified urgency to transfer funds urgently and is meant to be tailored for executives.

Vishing
The term is a combination of V-voice and Phishing and is usually used to steal credit card numbers or related data used in ID theft from individuals. Using a spoofed phone number and caller ID, the cybercriminal pretends to be catting on behalf of the victim's bank. The caller sous that there has been unusual activity on the victim's account and asks the victim to confirm their bank account details, including their mailing address, for updating proof of identification (KYC) by sending a link. This information is then used by the cybercriminal to commit online banking fraud.

Cyber-defamation
It occurs when defamation takes place with the help of computers and internet. If someone publishes a defamatory matter about someone on a website or posts any defamatory message on any digital media.
India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous once frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

Cyber-stalking
It is the use of internet and/ electronic communication devices by an individual or groups of individuals to harass another individual or groups of individuals or an organisation by false accusations, monitoring, transmission of threats, damage to data or equipment and gathering information for harassment. Online stalkers aim to start the interaction with the targeted victim directly through internet. Email and Chartrooms are the most common form of medium used to connect with the victim.
A 32-year-old man created a fake social media profile with obscene descriptions and photos of a woman and sent her obscene messages and photos after she ignored his messages on social media. A case was subsequently registered under Sections 67/67A (punishment for electronically transmitting obscenity in electronic form/sexual act in electronic form) of the Information Technology Act.

Computer sabotage/vandalism
The use of internet to obstruct the normal functioning of a computer system or networks through worms, viruses or logic bomb. Cyber vandalism is a program which performs malicious function such as extracting users' password or other confidential data or even erasing hard disk.

Password sniffers & Key logger
Password sniffers are programs that monitor and record the user id and passwords. A key logger is a type of spyware that monitors and records user keystrokes including the ability to record mouse clicks. They allow cybercriminals to read anything a victim is typing into their keyboard, including private data like passwords, account numbers, and credit card numbers. They can be installed manually or automatically without user's knowledge, such as by inserting a flash drive Into a USB slot or through a rootkit.

Transmitting virus
Computer virus is a software program that con infect legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves without the knowledge or permission of the users to potentially large numbers of programs on many machines.

- **Virus can be transmitted through the internet**

Virus Is Intentionally uploaded on internet server or distributed through email. The Internet server and hard disk gets infected with the virus. The virus then gets downloaded onto unsuspecting user if there are no anti-virus tool kit or outdated anti-virus tool kit is in the victim's computer.

- **Virus transmits through Stand-alone computer system**

When Virus infected pen drive or disk is loaded to the stand alone computer either intentionally or unintentionally and hard disk gets infected.

- **Virus can be transmitted through local network**

Virus is inserted in a legitimate program code and transmitted via data communication links to another node on the network. Virus then spreads itself to another nodes on the network.

Salami Attack

To commit a financial crime, an alteration is made so insignificant that it would go unnoticed. For example, if a bank employee inserts a program onto the bank server to deduct small amount of money make an unauthorised debit to bank account holders account and credit it to his fictitious bank account, he will be siphoning off a sizeable amount every month.

Theft of computer system and Internet time theft: This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer. Internet time theft occurs when an unauthorised person uses the Internet hours paid for by subscriber by hacking or gaining access by illegal means without the knowledge of the subscriber.

Intellectual Property Theft

Intellectual property rights means the ownership rights in intangible assets like software, source code, trade secrets, copyrights, and trade-marks. When the rights of an owner of an intellectual property right is deprived off either wholly or partially, it is called as intellectual property theft. There are many instances of piracy in the digital world since the advent of internet revolution. Online piracy or software piracy is the practice of downloading and distributing copyrighted works digitally without permission, such as music or feature films or software.

The Hyderabad Court in a land mark judgement convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software (Parthasarathy Pati case 16th March 2003).

Web Jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

Online Frauds

Online frauds are fraudulent activities such as an identity theft, financial frauds like online games or lotteries, free vacation.

Online Job frauds

It involves misleading people who require a job by promising them a better job with higher pay while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

- **SIM swapping or SIM Jacking**

It is a fraudulent way of gaining access to someone's mobile number. It happens when a criminal convinces cellular provider to transfer victim's phone number to a different SIM (Subscriber Identity Module) card, usually one in their possession. If they succeed, victim will automatically at a disadvantage.

- **Crypto currency frauds**

Crypto currency, such as bit coin, is different from digital currency. It uses blockchain for verification and does not run through financial institutions, so it is harder to recover from theft.

- **Fake crypto currency exchanges**

Scammers may lure investors in with promises of a great crypto currency exchange. But in reality, there is no exchange and the investor does not know it is fake until after they lose their deposit

- **Ponzi schemes**

To get fresh crypto currency investors, crypto currency scammers will lure new investors with bit coin.

- **Bit coin investment schemes**

As part of the scheme, the so-called investment managers claim to have made millions investing in crypto currency and promise their victims that they will make money with Investments. To get started, the scammers request an upfront fee. Then, instead of making money, the thieves simply steal the upfront tees. The scammers may also request personal identification information, claiming it's for transferring or depositing funds, and thus gain access to a person's crypto currency.

Conclusion

A broad overview about cybercrime and its various types have been explained in the above paragraphs. Various types of cybercrimes existing and new types of cybercrimes are happening every second in India and other parts of the globe. We should be aware of the latest cyber scams and cyber frauds that are happening and necessary internal controls should be designed to protect the organisation and individuals from falling victim to it. As the technology is growing at mind-blowing pace post pandemic, many more new types of cybercrimes will emerge since fraudsters are always ahead in the conning game. The ugly or negative side of proliferation of digital technologies is being witnessed every day. So, we need to think about it urgently and have safeguards against these types of Cyber Crimes and Frauds.

References

1. Chaturvedi SK, Baranwal Shradha. Cyber Crimes: Issues, Policy, Regulations and Developments, Satyam Law International, Delhi, 2023.
2. Dasgupta M. Cyber Crime in India: A Comparative Study, Eastern Law House, Lucknow, 2009.
3. Fatima, Talat. Cyber Crimes, Eastern Book Company, Lucknow, 2021.
4. Khubalkar, Deepti. Cybercrime Laws in India, University Book House Pvt. Ltd., Jaipur, 2019.
5. Konsam Tunicha, Verma Sandhya. Cyber Crime in India: Problem and Law related to Cyber Crime, Journal of Emerging Technologies and Innovative Research,2021:8(7):614-621.
6. Meena, Deepti, Mehra, Sarita Dehariya, Samadhiya, Priyansh, *et al*. Cyber Crimes in India, Book Rivers, Lucknow, 2024.
7. Pandit, Rahul. Cyber Crime in India: Trends, Challenges and Solutions, Notion Press, Chennai, 2024.
8. Thakur, Deshant Singh, Mitra, Ananyo, Roy, Souvik, *et al*. Emerging Trends in Cyber Crimes and Cyber Laws in India, Repro Books Limited, Mumbai, 2023.
9. www.legalserviceindia.com