



**RV College of  
Engineering®**

*Go, change the world*

# **22EM1C07-Introduction to Cyber Security**

## **UNIT- I**

### **Chapter-2: Introduction to Cyber Crime**

#### **Text Book:**

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011, Reprint 2022, ISBN:978-81-265-2179-1.

**Course Incharge: Dr. Praveena T**

**Department of Computer Science & Engineering (Cyber Security)**

**RV College of Engineering, Bangalore-560059**

Unit-I	8 Hrs
<b>Introduction to Cyber Space</b> History of Internet, History and evolution of Information Security and cyber-Security, introduction to cyber space and information security, computer ethics and security policies.	
<b>Introduction to Cybercrime</b> Definition and Origins of the Word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives. Different Types of Cyber Crimes, Scams and Frauds	

← → ↻ ncrb.gov.in/en

भारत सरकार  
GOVERNMENT OF INDIA

गृह मंत्रालय  
MINISTRY OF HOME AFFAIRS

Login SKIP TO MAIN CONTENT T T G+ ENGLISH हिन्दी

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो  
NATIONAL CRIME RECORDS BUREAU  
Empowering Indian Police with Information Technology

Citizen's Charter Contact us Feedback

Search, Keyword, Phrase Q

Home About us + Divisions + Publications + Citizen Services + Notifications + RTI Nodal Officer's Section +

**National Crime Records Bureau**  
**Ministry of Home Affairs**  
**4<sup>th</sup> Conference**  
**on**  
**Good Practices in CCTNS/ICJS**  
**December 15-16, 2022**  
Crime Statistics | CCTNS | NAFIS | ICJS | Cri-MAC | Cy-Train | NCRP

DEEPAK M DAMOR  
Joint Director, BUREAU

VIVEK GOGIA  
DIRECTOR, BUREAU

AJAY KUMAR MISHRA  
MINISTER OF STATE (HOME)

ARCHANA RAMASUNDARAM  
DEPUTY DIRECTOR, BUREAU

SANJAY MATHUR  
Joint Director, BUREAU

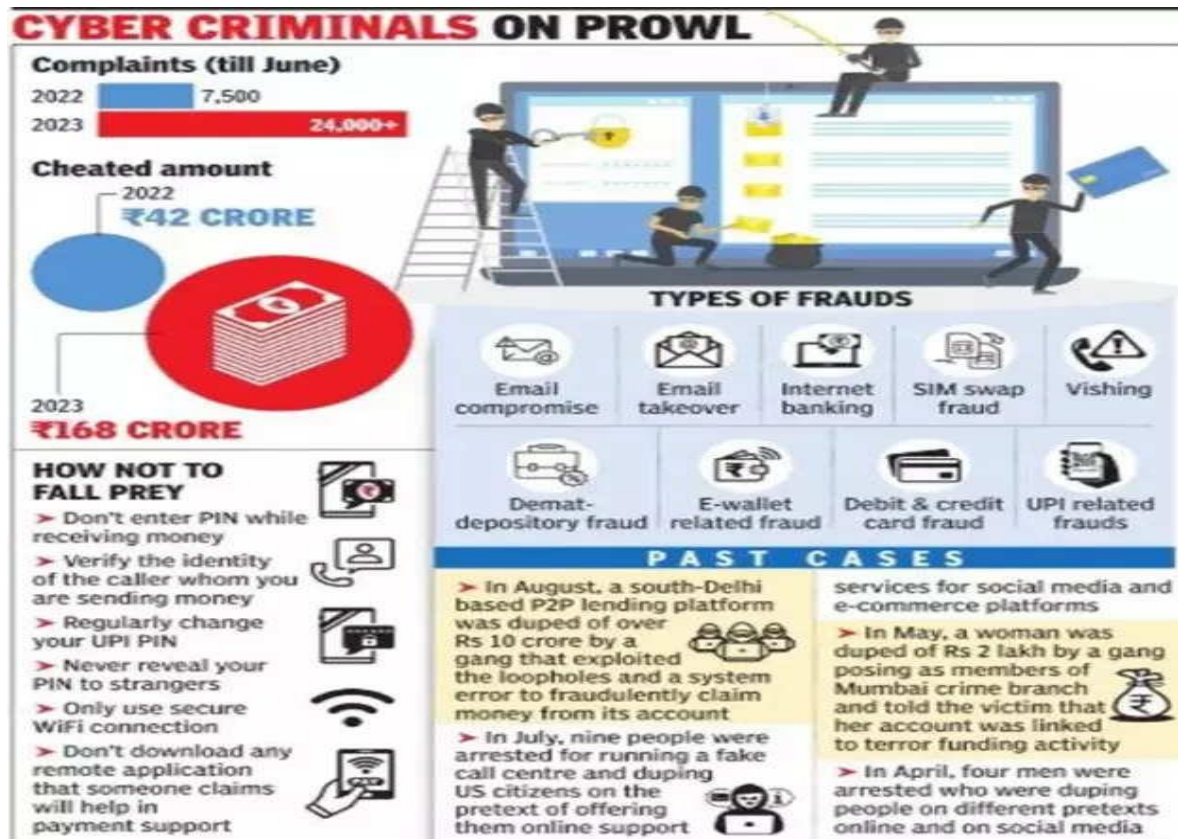
21:41

Source: <https://ncrb.gov.in/en>



<https://ncrb.gov.in/crime-in-india.html>

<https://www.adda247.com/upsc-exam/crime-rate/>



## Cyber crimes soar in Delhi, complaints jump 200% in 2023

Over 24,000 complaints were registered with the Delhi Police till June. During the same period in 2022, the cops had received 7,500 complaints.

TOI-Online

Updated On Aug 16, 2023 at 08:33 AM IST



Preliminary probe data showed that most of these frauds originated in Mewat (Haryana) and the infamous Jamtara (Jharkhand).

Cyber fraud complaints in Delhi so far in 2023 increased by 200% over the same period in the previous year, a ToI report said on August 15.

Over 24,000 complaints were registered with the Delhi Police till June. During the same period in

2022, the cops had received 7,500 complaints.



## Bengalureans lost ₹470 crore in cyber crimes in 2023

Police recover ₹28.4 crore, freeze ₹201.8 crore

October 11, 2023 10:54 am | Updated 10:56 am IST - Bengaluru

THE HINDU BUREAU

 COMMENTS  SHARE

 READ LATER



The cases include a variety of online frauds. | Photo Credit: Illustration by Satheesh Vellinezhi

Bengaluru recorded 12,615 cyber crime cases with a total loss of ₹470.05 crores till September-end 2023.

[Article:67404242.ece](#)

Of this, city police managed to recover ₹28.4 crore and froze ₹201.8 crore in various bank accounts. The police managed to return ₹27.6 crore to the rightful owners and are waiting for consent from courts to return the rest of the money, a police officer said.

The cases include a variety of online frauds, like online job fraud, debit or credit card fraud, gift fraud, loan app fraud, bitcoin cases, sextortion, data theft, matrimonial fraud, card skimming, email spoofing, lottery fraud, online gaming fraud, and SIM cloning.

## Cyber attacks targeted 36 government websites in 2023

**In the first half of 2023, 36 government websites experienced hacking incidents, and over 4.29 lakh cyber security incidents related to financial institutions were recorded, according to data shared by Minister of State for Electronics and IT Rajeev Chandrasekhar.**






As many as 36 websites of ministries and departments under the central and various state governments faced hacking incidents in the first six months of 2023, Parliament was informed on Wednesday.

Cyber security watchdog CERT-In tracked these incidents.

According to data shared by the Minister of State for Electronics and IT Rajeev Chandrasekhar in Lok Sabha, a total of 1,12,474 cyber security incidents have been tracked by CERT-In.


[Accessibility Options](#) | [Sitemap](#) | [Contact Us](#)



Enhancing Cyber Security in India





**Indian Computer Emergency Response Team**


Ministry of Electronics and Information Technology  
Government of India



सत्यमेव जयते

[HOME](#) | [ABOUT CERT-In](#) | [KNOWLEDGEBASE](#) | [TRAINING](#) | [ADVISORIES](#) | [VULNERABILITY NOTES](#) | [CYBER SECURITY ASSURANCE](#)










समृद्धि का नया भारत

समृद्धि कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE




Sabka Swachh  
Sabka Vikas  
Sabka Vishwas  
Sabka Prayas



**Swachhata Hi Seva**

15 September to 2 October 2023  
Garbage Free India




**Digital India**  
Power To Empower

साइबर स्वच्छता केन्द्र


CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre


Full Member




Operational Member



Accredited Member



Global Research



**Home - Vulnerability Notes**

---

**CERT-In Vulnerability Note CIVN-2022-0363**  
**Multiple Vulnerabilities in Tacitine Firewall**

Original Issue Date: September 20, 2022

Severity Rating: **CRITICAL**

Software Affected

- Tacitine Firewall EN6200-PRIME QUAD-35 versions 19.1.1 to 22.20.1
- Tacitine Firewall EN6200-PRIME QUAD-100 versions 19.1.1 to 22.20.1

**Overview**

Multiple vulnerabilities have been reported in Tacitine Firewall, which could allow an unauthenticated remote attacker to execute arbitrary commands, perform session fixation and view sensitive information on the targeted device.

**Description**

These vulnerabilities exist in Tacitine Firewall due to improper control of code generation, session management and insecure design in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit these vulnerabilities by sending specially crafted http requests on the targeted device.

Successful exploitation of these vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary commands, perform session fixation and view sensitive information on the targeted device.

**Credit**

This vulnerability is reported by Sreedev Kumar from Crowe India.

**Solution**

Update Tacitine Firewall to the latest software version 22.21.2.

- As per the cyber crime data maintained by the **National Crime Records Bureau (NCRB)** <https://ncrb.gov.in/en>
- According to **NCRB**, the police have recorded under both the **Information Technology (IT)** Act as well as the **Indian Penal Code (IPC)**.
- **58.6%** of the offenders were in the age **group 18–30 years**, **31.7%** of the offenders were in the age group **30-45 years** and **remaining reported offenders whose age was below 18 years.**
- Awareness and education, labs, research centres

- Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping.
- Fraud is the **intentional deception** of a person or group.
- Internet fraud includes any scheme using **Web sites, chat rooms, and email to offer nonexistent goods and services to consumers or to communicate false information to consumers.**
- Most scams are done by **e-mail**- critical information like usernames, passwords, credit card information, or other types of account information.

- hindering the **economic** and **social development of any nation**.
- Cyber fraud can also destroy our good and morally sound culture.

- Cybercrime in a narrow sense (computer crime): **Any illegal behavior directed by means of electronic operations** that targets the security of computer systems and the data processed by them.
- Cybercrime in a broader sense (computer-related crime): **Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.**
- Computer-related crime is considered as **any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.**



- A wide variety of **scams operate in the online environment**, ranging from fraudulent lottery schemes, travel and credit-related ploys, modem and web page hijacking, and identity theft (ID theft)
- Many online scams **originate in spam messages**.
- the “**advance fee fraud**” format of requiring up-front payment or investment on the promise of **high returns that are never forthcoming**.
- **Spam is a key tool for the spread of ID theft**

- “look alike” websites where users are tricked into divulging personal information which can be used to access and illegally transfer money out of the victim’s bank account(s)
- These attacks are continually becoming more sophisticated.
- Other variants of fraud rely on the use of identity stolen through technological methods.
- “key stroke” loggers and other programs to steal information stored on, entered into, or received by these devices.

According to the survey,

- 66% of Indian online adults have been a **victim of cyber fraud in their lifetime**. In the past 12 months, 56% of online adults in India have experienced cyber fraud.
- As per the report, at least **1,15,000 people fall prey to cyber fraud every day, while 80 per minute** and more than one per second leading to a rise in the average direct financial cost per victim to around Rs10,500.
- The cybercriminals have now **shifted their focus to the increasingly popular social platforms**. One in three adults online Indians (32%) have been either social or mobile cybercrime victims.

- While most internet users delete suspicious emails and are careful with their personal details online.
- 25% don't use complex passwords or change their passwords frequently and 38% do not check for the padlock symbol in the browser before entering sensitive personal information.
- Online adults are also unaware of the evolution of most common forms of cybercrime. In fact, 68% of adults do not know that malware can operate in a discreet fashion, making it hard to know if a computer has been compromised

- Setup an e-security program for your business.
- Ensure your security program facilitates confidentiality, integrity and availability.
- Identify the sources of threats to your data from both internal and external sources.
- must have provisions to maintenance and upgrades of your systems.
- Administrators have access to all files and data.
- Roles for security should be defined, documented, and implemented for both your company and external contractors.
- Establish a security awareness program for all users.
- **Maintain logs** of all possible activities that may occur on your system.
- User accounts should **not be shared**.

- Employee user accounts **must be disabled or removed** when no longer needed.
- Ensure network security from external sources by installing **firewalls and intrusion detection** systems.
- Allow remote access to employees only through **secure communication channels like SSL or VPN.**
- Install **antivirus software** on all desktops and servers.
- Create a **data backup and disaster recovery plan** in case of unforeseen natural calamities.
- Ensure **back-up procedures** are in place and tested.
- Ensure back-up procedures include **all the critical** as well as **back office data** such as finance, payroll etc.
- **Incident response** is the ability to identify, evaluate, raise and address negative computer related security events.
- In case of an incident, **do not panic, and continue to save logs.**
- **Incident response** - Take a backup of the **affected system** and **notify the authorities.**



1. Cyber pornography
2. Sale of illegal articles
3. Online gambling
4. Intellectual Property crimes
5. Email spoofing
6. Forgery
7. Cyber Defamation:
8. Cyber stalking
9. Unauthorized access to computer systems or networks
10. Theft of information contained in electronic form
11. Email bombing

12. Data diddling
13. Salami attacks
14. Denial of Service attack
15. Virus / worm attacks
16. Logic bombs
17. Trojan attacks
18. Internet time theft
19. Web jacking
20. Theft of computer system
21. Physically damaging a computer system

This would include **pornographic websites; pornographic magazines produced using computers** (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Ex. (Delhi Public School case)

- sale of **narcotics, weapons and wildlife** etc.,
- by **posting information on websites, auction websites, and bulletin boards or simply by using email communication.**
- E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

- There are millions of websites; all hosted on **servers abroad, that offer online gambling.**
- **money laundering.**

Ex. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a **website and an email address on the Internet with the address 'eurolottery@usa.net.'** Whenever accessed, the site would name him as the beneficiary of **the 12.5 million pound.**

After confirmation a Telugu newspaper published this as a news. He collected huge sums from the **public as well as from some banks for mobilization of the deposits in foreign currency.** However, the fraud came to light when a **cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced.** Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffield, London stating that a term deposit of 12.5 million was held in his name.

- These include software piracy, copyright infringement, trademark violations, theft of computer source code etc.
- In other words this is also referred to as cyber squatting.
- Ex. Satyam Vs. Siffy is the most widely known case.



- A spoofed email is one that **appears to originate from one source but actually has been sent from another source.**

E.g. Gauri has an e-mail address [gauri@indiaforensic.com](mailto:gauri@indiaforensic.com). Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances.

Email spoofing can also cause monetary damage.

Ex. Recently, a branch of the **Global Trust Bank** experienced a run on the bank.

Numerous customers decided to withdraw all their money and close their accounts.

- Counterfeit currency **notes, postage and revenue stamps**, mark sheets etc can be forged using sophisticated computers, printers and scanners.
- These are made using **computers, and high quality scanners and printers**.
- In fact, this has becoming a **booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.**

- This occurs when defamation takes place with the help of computers and / or the Internet.

E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

- The Oxford dictionary defines stalking as “pursuing stealthily”.
- Cyber stalking involves following a **person’s movements across the Internet by posting messages** (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

## 9. Unauthorized access to computer systems or networks

---

*Go, change the world*

- This activity is commonly referred to as **hacking**.
- “unauthorized access” interchangeably with the term “hacking”.



- This includes information stored in **computer hard disks**, removable storage media etc.



- Email bombing refers to sending a **large number of emails to the victim resulting in the victim's email account** (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
- **sending e-mail still their servers crashed.**

- This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
- Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

- These attacks are used for the **commission of financial crimes**.
- The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.
- E.g. a **bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5a month)** from the account of every customer.
- **sizeable amount of money being transferred into his account every Saturday.**

- This involves flooding a **computer resource with more requests** than it can handle.
- This causes the resource (e.g. a web server) to **crash thereby denying** authorized users the service offered by the resource.
- **sending excessive demands to the victim's computer(s), exceeding** the limit that the victim's servers can support and making the servers crash.
- Denial-of-service attacks have had an **impressive history having, in the past, brought down websites** like Amazon, CNN, Yahoo and eBay!

- 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.

- These are event dependent programs.
- This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.
- E.g. even some viruses may be termed logic bombs because they **lie dormant all through the year and become active only on a particular date** (like the Chernobyl virus).

- A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

- This connotes the usage by an **unauthorized person** of the Internet hours paid for by another person.



- 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.**

- This type of offence involves the **theft of a computer, some part(s) of a computer or a peripheral attached** to the computer.

- This crime is committed by **physically damaging a computer** or its peripherals.
- This is just a list of the known crimes in the cyber world.
- The unknown crimes might be far ahead of these, since the **lawbreakers are always one-step ahead of lawmakers.**

- i. **Insiders** - Disgruntled employees and ex-employees, spouses, lovers
- ii. **Hackers** - Crack into networks with malicious intent
- iii. **Virus Writers** - Pose serious threats to networks and systems worldwide
- iv. **Foreign Intelligence** - Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country
- v. **Terrorists** - Use to formulate plans, to raise funds, propaganda

- world is becoming **more and more digitally sophisticated** and so are the crimes.
- Transactional **with e-business, e-commerce, e-governance and e-procurement** etc.
- **All legal issues related to internet crime** are dealt with through cyber laws.
- In today's highly digitalized world, almost everyone is affected by cyber law.

- As globalization and computerization grew rapidly in India, cyber regulations began to take shape.
- Every year, a startling number of cybercrimes are reported in India, and the problem is only getting worse. This is due to India's digital transformation, which has increased the pool of naive targets for cyber con artists. This necessitates having a fundamental understanding of the regulations that apply to India's cyberspace.
- Year 2008 saw an amendment to India's Cyber Laws, often known as the Information Technology Act, which added cybercrimes relating to banking and financial operations.

For understanding Cyber Law in India, firstly, we have to discuss cyber law in simple terms-

## What do you mean by Cyber Law?

The area of the legal system that is related to legal informatics and that regulates the electronic exchange of information, e-commerce, software, and information security is known as **cyber law**, also known as **Internet law** or **cyber law**.

- It is connected to legal informatics and electronic components like computers, software, hardware, and information systems.
- It covers a wide range of themes, including online privacy and freedom of expression, as well as access to and use of the Internet, which includes several subtopics.

India has laws against cybercrime, which is any crime committed using technology and a computer as a tool. Citizens are prevented from sharing private information with strangers online by cybercrime laws. The IT Act 2000, which was passed and revised in 2008 to cover many types of offenses under Indian cyber law, has been in effect since the establishment of cyber laws in India.

- ☐ Internet law and regulation are collectively referred to as "**cyber law**" in this context. Cyber laws cover anything that has to do with, is connected to, or results from legal matters or any citizen activity in cyberspace.
- ☐ Legal issues relating to the usage of network information technology and devices' distributive, transactional, and communicative features are covered by cyber law. It covers all of the laws, regulations, and constitutional clauses that apply to networks and computers.



Following are the major advantages of cyber law:

- ☐ Utilizing the legal framework, the Act provides, businesses can now conduct e-commerce.
- ☐ In the Act, digital signatures have been given legitimacy and authorization.
- ☐ It has made it possible for corporate organizations to issue digital signature certificates and operate as certifying authorities.
- ☐ It paves the way for e-government by enabling the government to publish alerts online.
- ☐ It allows businesses or organizations to electronically submit any forms, applications, or other documents to any offices, authorities, bodies, or agencies that are owned or managed by the appropriate government using any e-forms that may be specified by that government.
- ☐ The IT Act also addresses the crucial security concerns that are essential to the success of electronic transaction.

- ☐ On October 17, 2000, the Information Technology Act of 2000 went into effect. This Act is applicable to all of India, and its provisions also apply to any violation or offense committed by any individual, regardless of nationality, even outside the Republic of India's territorial authority.
- ☐ Such an offense or contravention shall include a computer, computer system, or computer network located in India that is subject to the provisions of this Act. The extraterritorial applicability of the provisions of the IT Act 2000 is provided by Section 1(2) read in conjunction with Section 75.
- ☐ The Information Technology Act of 2000 in India has made an effort to include legal ideas found in other information technology-related laws that have already been passed in other nations as well as different information technology law-related guidelines.
- ☐ The Act recognizes electronic signatures and grants electronic contracts legal validity. Defamation (sending offensive communications), hacking, data theft, virus spreading, identity theft, pornography, child pornography, and cyber terrorism are now all considered crimes under this modern legislation.

Cyber laws cover the following statutes, rules, and guidelines.

- ☐ Information Technology Act, 2000
- ☐ Information Technology (Certifying Authorities) Rules, 2000
- ☐ Information Technology (Security Procedure) Rules, 2004
- ☐ Information Technology (Certifying Authority) Regulations, 2001
- ☐ The Indian Evidence Act, 1872
- ☐ The Bankers Books Evidence Act, 1891

Cyber law includes regulations on:

- ❖ Online crimes
- ❖ Digital and electronic signatures
- ❖ Intangible assets
- ❖ Preserving the privacy of data



- ☐ **Fraud** – Cyber laws are essential to consumers' protection against online fraud. Legislation is created to stop online financial crimes, including credit card theft, identity theft, and others. Identity thieves may be charged as accomplices or as state criminals. They might also run into a victim-driven civil lawsuit. Cyber attorneys work to both defend and prosecute clients accused of online fraud.
- ☐ **Copyright** – Copyright violations have become easier because of the internet. Copyright infringement was all too common in the early days of online communication. To file a lawsuit to impose copyright protections, businesses and individuals both need lawyers. Cyber law defends people's and businesses' rights to make money off of their creative works in the domain of copyright violation.
- ☐ **Defamation** – Many employees use the internet to express themselves. Using the internet to spread untrue information might cross the line into defamation. Laws against defamation are civil laws that protect people from false public statements that might hurt someone's reputation or a business. Defamation legislation refers to when individuals use the internet to make claims that are illegal under civil laws.

- ☐ **Harassment and Stalking** – Criminal laws that prohibit stalking and harassment can occasionally be broken by online words. There is a violation of both civil and criminal statutes when someone repeatedly posts threatening comments about another individual online. When stalking occurs online or through other electronic communication, cyber lawyers both prosecute and defend the victim.
- ☐ **Freedom of Speech** – An essential component of internet law is freedom of speech. Freedom of speech rules also let people express their opinions, despite the fact that cybercrime laws prohibit specific acts online. The boundaries of free expression, particularly those imposed by laws against obscenity, must be discussed with clients by cyber attorneys. In cases where it is disputed whether a client's acts qualify as free speech, cyber lawyers may also stand up for their clients.

- ☐ **Trade secrets** – Cyber laws are frequently used by businesses doing online transactions to safeguard their trade secrets. For instance, the algorithms used by Google and other online search engines to generate search results are developed over a long period of time. They also devote a lot of work to creating other features, including search services for flights, intelligent assistance, and maps. Cyber security laws support these businesses in taking legal action when required to safeguard their trade secrets.
- ☐ **Contract and Employment** – Cyber law is used each time a user clicks a button acknowledging their agreement to a website's terms and conditions. Every website has terms and conditions relating to privacy issues in some way.

- Almost **all transactions** in shares are in demat form.
- Almost all companies **extensively depend upon their computer networks** and keep their valuable data in electronic form.
- **Government forms** including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are **increasingly using credit cards** for shopping.
- Most people are using **email, cell phones and SMS messages** for communication.
  - Even in "**non-cyber crime**" cases, important **evidence is found in computers / cell phones**.
  - Digital signatures and e-contracts are fast replacing conventional methods of transacting business.



- Access
- Addressee
- Affixing Electronic Signature
- Asymmetric Crypto System
- Certifying Authority
- Communication Device
- Computer
- Computer Network
- Computer Resource
- Computer System
- Cyber café
- Cyber Security
- Data

- Digital Signature
- Electronic Form
- Electronic Record
- Electronic signature
- Function
- Information
- Intermediary
- Key Pair
- Originator
- Private Key
- Public Key
- Secure System
- Subscriber

## Access

- Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, **computer system or computer network**.

## Addressee

- Person who is **intended by the originator** to receive the electronic record but does **not include any intermediary**.

## Affixing Electronic Signature

- adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of **Electronic Signature**.

## Asymmetric Crypto System

- secure key pair consisting of a **private key for creating a digital signature** and a public key to **verify the digital signature**.

## Certifying Authority

- Person who has been **granted a license to issue** a Electronic Signature Certificate

## Communication Device

- Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to **communicate, send or transmit any text, video, audio, or image**.

## Computer

- any **electronic, magnetic, optical** or other **high-speed data processing** device or system

## Computer Network

- interconnection of **one or more Computers** or Computer systems or Communication device

## Computer Resource

- computer, communication device, computer system, **computer network, data, computer database or software.**

## Computer System

- **Device or collection of devices**, including input and output support devices

## Cyber café

- Facility from **where access to the Internet** is offered by any person in the ordinary course of business to the members of the public.

## Cyber Security

- Protecting **information, equipment, devices, computer, computer resource, communication device and information** stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

## Data

- Representation of **information, knowledge, facts, concepts** prepared in a formalized manner

## Digital Signature

- Authentication of **any electronic record by a subscriber** by means of an electronic method or procedure.

## Electronic Form

- Any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

## Electronic Record

- data, record or data generated, image or sound stored, received or sent in an electronic form.

## Electronic signature –

- Authentication of any electronic record by a subscriber by means of the electronic technique

## Function

- in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer

## Information

- includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

## Intermediary

- Any particular electronic records, means any person who on behalf of another person receives, stores or transmits

## Key Pair

- An asymmetric crypto system

## Originator

- Person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

## Private Key

- key pair used to create a digital signature.

## Public Key

- key pair used to verify a digital signature and listed in the Digital Signature



## Secure System

- computer hardware, software, and procedure
- secure from unauthorized access and misuse
- provide a reasonable level of reliability and correct operation;
- reasonably suited to performing the intended functions; and
- adhere to generally accepted security procedures.

## Subscriber

- Means a person in whose name the Electronic Signature Certificate is issued.

- In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000.
- purpose of the Act is to provide **legal recognition to electronic commerce** and to **facilitate filing of electronic records** with the Government.

Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

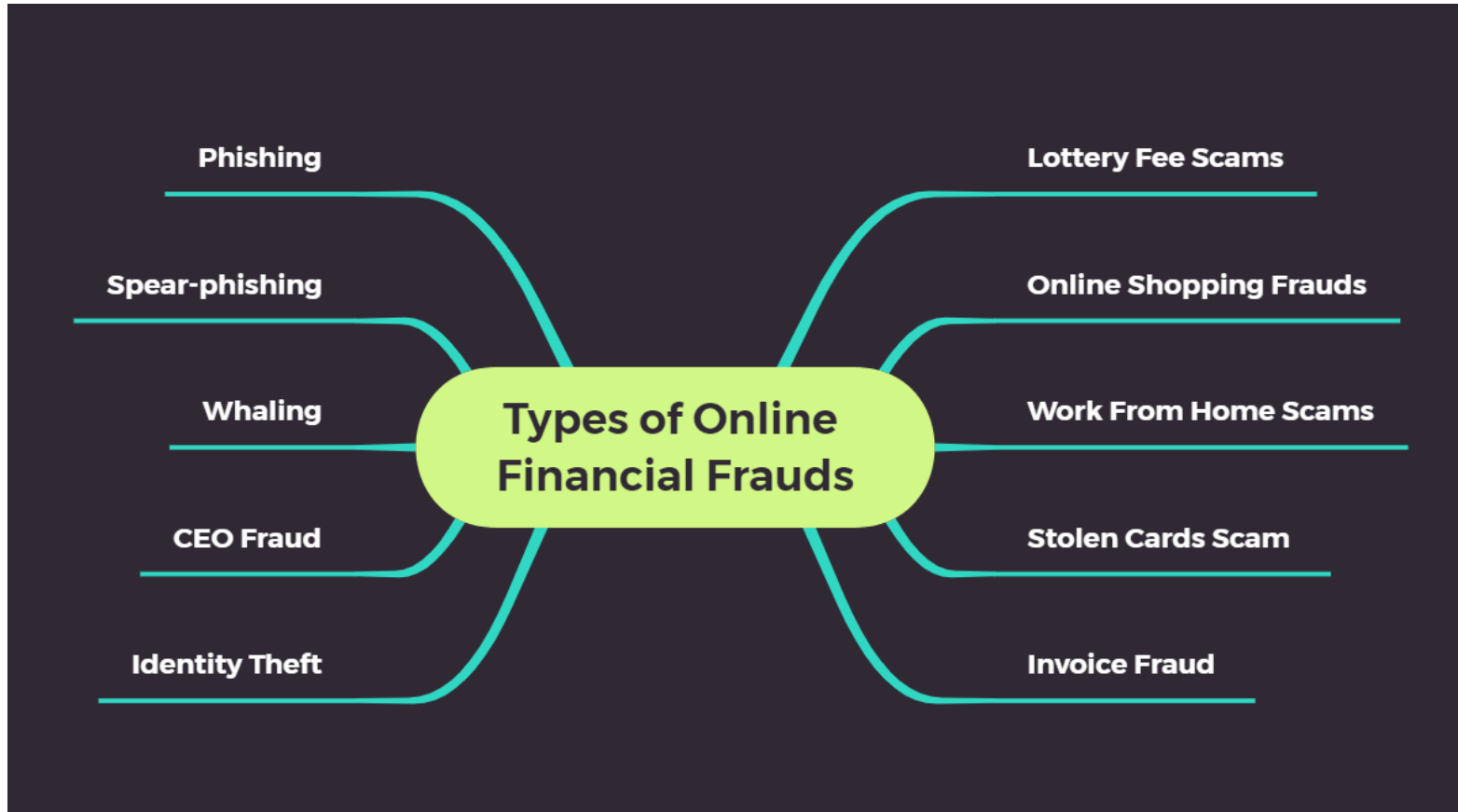
- India has an extremely **detailed and well-defined legal system** in place.
- The existing laws of India, even with the most benevolent and liberal interpretation, could **not be interpreted in the light of the emerging cyberspace**, to include all aspects relating to **different activities in cyberspace**.
- None of the existing laws **gave any legal validity or sanction** to the activities in Cyberspace.
- Internet requires an **enabling and supportive legal infrastructure** in tune with the times.

- The term '**digital signature**' has been replaced with '**electronic signature**' to make the Act more technology neutral.
- A new section has been inserted to define '**communication device**' to mean **cell phones, personal digital assistance or combination of both** or any other device used to communicate, send or transmit any text video, audio or image.
- A new section has been added to **define cyber cafe** as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- A new definitions has been **inserted for intermediary**.

- a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- b) The Information Technology (Electronic Service Delivery) Rules, 2011
- c) The Information Technology (Intermediaries guidelines) Rules, 2011
- d) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011
- e) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009
- f) The Cyber Appellate Tribunal (Procedure for investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009

- g) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009
- h) The Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009
- i) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009
- j) The Information Technology (Use of electronic records and digital signatures) Rules, 2004
- k) The Information Technology (Security Procedure) Rules, 2004

- l) The Information Technology (**Other Standards**) Rules, 2003
- m) The Information Technology (**Certifying Authority**) Regulations, 2001
- n) Information Technology (**Certifying Authorities**) Rules, 2000





## 10 Popular Internet SCAMS





<https://reportfraud.ftc.gov/#/>



Search FAQs on ReportFraud.ftc.gov



FAQs

Update Report

Español

Report Now →

⚠ COVID-19 scams? [Report here.](#)

⚠ Price gouging? [Report here.](#)

## Report to help fight fraud!

Report Now →

**Q1. What is the importance of Cyber Law in India?**

Ans. In India, the main goals of cyber law are the legal recognition and control of computerized transactions. Cyber law in India has a number of benefits. It gives legal status to electronic transactions and supports e-commerce in India.

**Q2. Which is the first cyber law in India?**

Ans. The Information Technology Act 2000 is the first cyber law in India.

**Q3. What are the types of cyber laws?**

Ans. Cybercrime law includes substantive, procedural and preventive law.

**Q4. Who is the founder of Cyber Law?**


Ans. Karuppannan Jaishankar is the founding Principal Director & Professor of Criminology and Crime Sciences at the International Institute of Crime & Security Sciences (IICSS).

**Q5. What is cyber law called?**

Ans. Cyber Law is also called as digital law.

<https://www.meity.gov.in/content/cyber-laws>

<https://meity.dashboard.nic.in/DashboardF.aspx>



**Ministry of Electronics & Information Technology**  
Government of India

Skip to main content / Screen Reader Access / [A](#) [A](#) / [A+](#) [A+](#) [A](#) / [f](#) [t](#) [b](#) हिन्दी /



Enter Your keywords 

[Home](#) [About MeitY](#) [Divisions](#) [Organisations](#) [RTI](#) [Notifications](#) [Azadi Ka Amrit Mahotsav](#)

**What's New**

**Know Your Minister**

**Performance Smartboard**

**Public Opinion and Public Grievances**

Your are here > [Home](#) > [Divisions](#) > [Cyber Laws Division](#) > [Cyber Laws](#)

## Cyber Laws



Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes.

✦ [Information Technology Act 2000\(IT Act 2000\) and its Amendment](#)

✦ [Notifications and Rules](#)