**Cyber Law**

**Cyber Law** also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

**According to the Ministry of Electronics and Information Technology, Government of India :**

*Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check [cyber crimes](https://www.geeksforgeeks.org/information-security-cyber-crime/).*

**Importance of Cyber Law:**

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

**Area of Cyber Law:**

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**   
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.
2. ***Copyright*:**   
   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.
3. ***Defamation*:**   
   Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone’s reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

1. ***Harassment and Stalking*:**

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication. 

1. ***Freedom of Speech*:**

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

1. ***Trade Secrets*:**

Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets. 

1. ***Contracts and Employment Law*:**

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns. 

**Advantages of Cyber Law:**

* Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.

* Digital signatures have been given legal validity and sanction in the Act.
* It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
* It allows Government to issue notifications on the web thus heralding e-governance.
* It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
* The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
* Cyber Law provides both hardware and software security.

**Cyber laws**, also known as internet laws or digital laws, are laws that govern the use of the internet and other digital technologies. These laws address a wide range of issues, including intellectual property, privacy, cybercrime, and liability for online activities. Cyber laws vary from country to country, but most countries have laws that address issues such as hacking, identity theft, and online fraud.

There are several key cyber laws that govern online activity and protect individuals and organizations from cybercrime. Some of the most important laws include:

1. **The Computer Fraud and Abuse Act (CFAA)**: This law criminalizes unauthorized access to computer systems and networks, as well as unauthorized access to sensitive information stored on those systems.
2. **The Electronic Communications Privacy Act (ECPA)**: This law regulates the interception and disclosure of electronic communications, including email and text messages.
3. **The Health Insurance Portability and Accountability Act (HIPAA)**: This law regulates the use and disclosure of protected health information (PHI) in electronic form.
4. **The Children’s Online Privacy Protection Act (COPPA)**: This law regulates the collection of personal information from children under the age of 13.
5. **The General Data Protection Regulation (GDPR)**: This EU regulation regulates the collection and processing of the personal data of EU citizens.
6. **The Personal Data Protection Bill (PDPB)**: In India, this bill regulates the collection, storage, and processing of personal data of Indian citizens.

# Cyber Crime

**Cybercrime** or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation’s security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

### **Classification of Cyber Crime:**

1. **Cyber Terrorism**

Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.   
In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

1. **Cyber Extortion**

Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

1. **Cyber Warfare**

Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

1. **Internet Fraud**

Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

1. **Cyber Stalking**

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims’ lives more miserable.

### Challenges of Cyber Crime:

1. **People are unaware of their cyber rights**

The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

1. **Anonymity-**  
   Those who Commit cyber crime are **anonymous**for us so we cannot do anything to that person.

1. **Less numbers of case registered-**

Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don’t register a case of cyber crime and this is major challenge for us as well as for authorities as well.

1. **Mostly committed by well educated people-**

Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very **technical**person so he knows how to commit the crime and not get caught by the authorities. 

1. **No harsh punishment**

In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

### **Prevention of Cyber Crime:**

Below are some points by means of which we can prevent cyber crime:

1. **Use strong password**

Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

1. **Use trusted antivirus in devices –**  
   Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.
2. **Keep social media private –**  
   Always keep your social media accounts data privacy only to your friends. Also make sure only to make friends who are known to you.
3. **Keep your device software updated –**  
   Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.
4. **Use secure network –**  
   Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.
5. **Never open attachments in spam emails –**  
   A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
6. **Software should be updated –**

Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.