Introduction to Cyber Law

In a Simple way, we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target: -using a computer to attack other computers.
  e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- The computer as a weapon: -using a computer to commit real-world crimes.
  e.g. Cyber Terrorism, IPR violations, Credit card frauds, Pornography etc.

Cyberlaw (also referred to as cyberlaw) is a term used to describe the legal issues related to using of communications technology, particularly "cyberspace", i.e. the Internet.

Cyberlaw in India

When the Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all-pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage in a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India.

Importance of Cyberlaw

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web, and Cyberspace. Initially, it may seem that Cyber laws is a very technical field and that it does not have any bearing on most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely because it is in the form of electronic records.

Internet Frauds

Internet fraud is a type of fraud which makes use of the Internet. This type of fraud varies greatly and appears in many forms. It ranges from E-mail spam to online scams. Internet fraud can occur even if partly based on the use of internet services and is mostly or completely based on the use of the internet.

The main types of internet fraud:

□ Stolen credit cards

Credit Card fraud across the internet is one of the more common examples of this type of crime. Some people fall prey to this type of scam because they are careless whilst others are duped by clever phishing schemes.

□ Emails

Used as intended, email is a great means of communication that can allow messages to be sent to huge numbers of people at virtually no cost. Unfortunately, this means that it is also an ideal medium for scam artists.

- Lotteries

Fake lottery scams will try to persuade you that you've won a huge amount of money in an online draw. People behind this fraud then try to trick you into revealing your personal information as you try to collect your winnings.

- Fake auctions

Buying and selling goods through internet auction sites is an extremely popular pastime for some, and a great means of doing business for others. Unfortunately, scam artists have seen the potential of infiltrating online auction sites. Internet auction fraud is one of the most common rip-offs on the net today.

- Untrustworthy Websites

A slightly newer form of internet fraud is the fake website. Cybercriminals have begun mimicking established websites and then tricking visitors into interacting with them as if they were the real deal.

Good Computer Security Habits

1. Create Strong Passwords

Passwords are usually the first, and sometimes only, protection against unauthorized access. They are the keys to your online kingdom, so keep these guidelines in mind.

Do not use your name, common phrases or words or acronyms that can be found in the dictionary—including foreign languages.

2. Lock your computer screen

You never know who might use your computer when you're not around, so it's important to lock your screen to prevent unauthorized access. In the office, a co-worker, guest or a service provider might view or use your unattended computer. This is an easy way for private information to become public.

3. Secure mobile devices from loss

While mobile devices such as smartphones, tablets, and laptops are valued for their portability, this convenience can become a security risk.

It's easy to lose or misplace these devices, so be sure to:

- Make a list of phone numbers and email addresses to report stolen or lost devices Use a hardware cable lock for your laptop, or store it in a locked drawer.
- Keep smartphones and tablets with you when in public
  Never put devices in your checked baggage when traveling

4. Protect data on mobile devices and removable media

Mobile devices and removable media, such as USB drives, enable us to easily share and transport information but can lead to the loss or misuse of data.

5. Identify URLs before clicking

Simply stated: think before you click. A malicious website that looks legitimate is a common method used by criminals. However, verifying the real destination is easy—just place your cursor over the displayed URL, and the true destination will reveal itself with a small pop-up. Don’t click if it looks suspicious.

6. Use public Wi-Fi safely

Public Wi-Fi is riskier than corporate or home Wi-Fi because you can’t determine its setup and security features. So, take extra precautions when using it.

□ Do not access sensitive personal accounts, such as financial accounts
□ Ensure websites use HTTPS and display a lock icon
□ Watch out for “shoulder surfing” from people and security cameras
□ Never use a public computer, such as one in a hotel lobby, to access personal information
□ Use only for general web browsing, e.g., weather forecasts and restaurant reviews.

7. Think before you post to social media

Social media provides a convenient, fun way to stay in touch with friends and family. But be cautious about what you post. Understand both personal and business risks, and take the following precautions:

□ Always comply with your company’s rules for business conduct
□ Ask friends and family to keep your private, personal information including relationships
□ Be cautious about participating in games and surveys or **clicking** on links suggested by others
□ Review and update your social media privacy and security settings often.