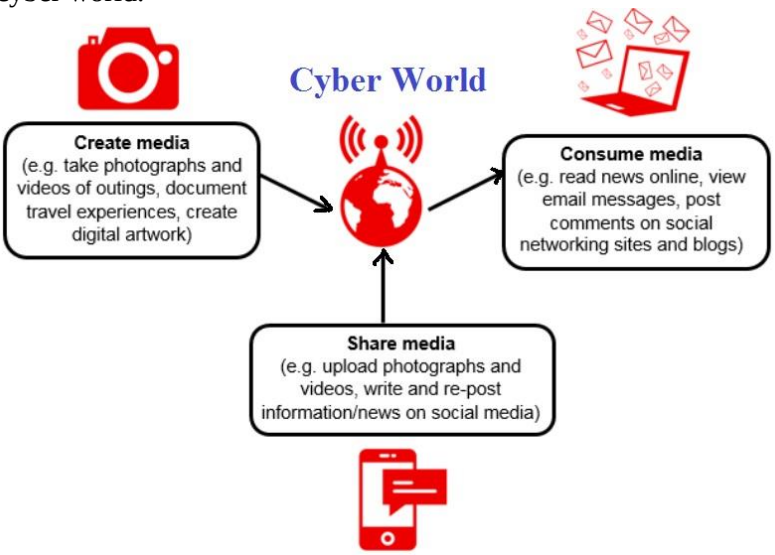
What is Cyber World?

The Cyber World, or cyberspace, is more than just the Internet. It refers to an online environment where many participants are involved in social interactions and have the ability to affect and influence each other. People interact in cyberspace through the use of digital media. The following figure shows an idea about the cyber world.



What is Cyber Law?

Generically, cyber law is referred to as the Law of the Internet. Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.

It is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace" or the “Internet”.

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.
- computer as a weapon :-using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

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 notification 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 by means of 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.

What is the Internet?

The Internet is a global network of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more. We can do all of this by connecting a computer to the Internet, which is also called “online”. When someone says a computer is online, it's just another way of saying it's connected to the Internet.

Again, the World Wide Web—usually called the Web, is a collection of different websites we can access through the Internet. A website is made up of related text, images, and other resources.

Online Resources:

In general, Web pages and documents on the Internet that provide useful information are called the online resources. While an online resource is typically data and educational in nature, any support software available online can also be considered a resource. Sometimes we can also say any resources those are accessible via the Internet and World Wide Web is online resources.

Information Security and Computer Security:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.

Information Security is not only about securing information from unauthorized access. It is basically the practice of preventing unauthorized access or use. Information can be physical or electronic one and it can be anything like our details like profile on social media, our data in mobile phone, our biometrics etc. Thus Information Security involves in so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

Information Security includes mainly three objectives:

- Confidentiality – means information is not disclosed to unauthorized individuals, entities and process.
- Integrity – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.
- Availability – means information must be available when needed.

Cyber Security Threats

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Different types of cyber security threats are mentioned below:

- Malware- Malware is malicious software such as spyware, ransom ware, viruses and worms.
- Emotet- It is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware.
- Denial of Service- A denial of service (DoS) is a type of cyber-attack that floods a computer or network so it can't respond to requests.
- Man in the Middle- A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction.
- Phishing- Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number.
- Password Attacks- With the right password, a cyber-attacker has access to a wealth of information.

UNIT-2

CYBER CRIMES:
Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most of the cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. It is very rear that cybercrimes aims to damage computers for reasons other than profit. These could be political or personal.

Cybercrimes are quite different from traditional crimes as they are often harder to detect, investigate and prosecute and because of that cybercrimes cause greater damage to society than traditional crimes. Cybercrime also includes traditional crimes conducted through the internet or any other computer technology.

Classification of Cybercrimes:
The cybercrimes may be broadly classified into four groups. They are:

1. **Crime against the Individuals**: Crimes that are committed by the cyber criminals against an individual or a person. A few cybercrimes against individuals are:
   - Harassment via electronic mails.
   - Dissemination of obscene material.
   - Cyber-stalking.
   - Defamation.
   - Indecent exposure.
   - Cheating.
   - Unauthorized control/access over computer system.
   - Email spoofing.
   - Fraud.

2. Crimes against Property: These types of crimes includes vandalism of computers, Intellectual (Copyright, patented, trademark etc.) Property Crimes, Online threatening etc. Intellectual property crime includes:
- Computer vandalism.
- Transmitting virus.
- Net-trespass.
- Unauthorized access / control over computer system.
- Internet thefts.
- Intellectual Property crimes- Software piracy, Copyright infringement, Trademark infringement.

3. Crime against Organization: Crimes done to threaten the international governments or any organization by using internet facilities. These cybercrimes are known as cybercrimes against Organization. These crimes are committed to spread terror among people. Cyber terrorism is referred as crimes against a government. Cybercrimes against Government includes cyber-attack on the government website, military website or cyber terrorism etc.
- Unauthorized access / control over computer system.
- Cyber terrorism against the government organization.
- Possession of unauthorized information.
- Distribution of Pirate software.

4. Crime against Society: Those cybercrimes which affects the society interest at large are known as cybercrimes against society, which include:
- Child pornography.
- Indecent exposure of polluting the youth financial crimes.
- Sale of illegal articles.
- Trafficking.
- Forgery.
- Online gambling.

The I.T Act 2000:

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The following are the important objectives of Information Technology Act, 2000:

- Grant legal recognition to E-Transactions
- Provide legal recognition to Digital Signatures for authentication
- Facilitate E-Filing of data and information
- Allow Electronic storage of data
- Grant recognition to maintenance of books of accounts in Electronic Form

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

Digital Forgery:

Forgery is the creation of a document which one knows is not genuine and yet projects the same as if it is genuine. Digital forgery (or digital tampering) is the process of manipulating documents or images for the intent of financial, social or political gain. Here, digital technology is used to forge a document, desktop publishing systems, color laser and ink-jet printers, color copiers, and images canners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

Cyber defamation:

Defamation means giving an "injury to the reputation of a person" resulting from a statement which is false. If anyone damages someone's reputation by the way of 'Slander' or 'Libel' one can sue for defamation. We can define the two terms as follows.

Libel – A statement that is defamatory and is published in a written form.

Slander – A defamatory statement spoken that means a verbal form of defamation.

The term 'Cyber Defamation' basically means publishing of false statement about an individual in cyberspace that can injure or demean the reputation of that individual. Cyber defamation involves defaming a person through a new and far more effective method such as the use of modern Electronic devices. It refers to the publishing of defamatory material against any person in cyberspace or with the help of computers or the Internet.

Cyber pornography:

Cyber Pornography means the publishing, distributing or designing pornography by using cyberspace. The technology has its pros and cons and cyber pornography is the result of the advancement of technology. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops; they even have access to upload pornographic content online. Cyber Pornography has become a global problem.

According to different journals and publications

- 30% of Internet content is porn.
- Almost 20% of the mobile phone searches are for porn.
- 28,258 users watch porn every second.
- 90% of boys and 60% of girls watch porn by the time they turn 18.

Child pornography is an illegal act in India. Information Technology Act, 2000 & Indian Penal Code, 1860 gives protection against the child pornography. Child refers to the person who is below the age of 18 years. Section 67B of the IT Act, 2000 makes it publishing, transmitting, viewing or downloading child pornography illegal.

Hacking and Cracking: