Computer science

Computer security

- Definition of Security
- Software Licenses
- Intellectual Property (IP)
- Electronic Intrusion
- Malware
- Viruses
- Protection from virus

Computer science

❖ Definition of Security

- Security has always been an overriding concern of human kind. For many organization, information plays a very important role in running business.
- Therefore, it becomes necessary to safeguard information from reaching the illegal hands. When data takes the shapes of digital form, a different security procedure is required. This branch of security is called computer security.

Computer science

- **Security can be defined as the protection of assets.**

- There are three main aspects to security:

  1.Prevention

  2.Detection

  3. Reaction

Computer science

❖ Software Licenses

- ✓ is a document that provides legally binding guidelines for the use and distribution of software and also defines the rights of the software producer and of the end-use.
- ✓ Software licenses typically provide end users with the right to one or more copies of the software.
- ✓ There are different types of licenses and licensing contracts, and different vendors may use different terms to describe their licenses.

Computer science

- **Types of licenses**

1. Proprietary license
2. General Public License
3. Workstation licenses
4. Concurrent use license
5. Site licenses
6. Perpetual licenses
7. Non-perpetual licenses
8. License with Maintenance

Computer science

Intellectual Property (IP)

- Intellectual property (IP) refers to creations of the human mind or the fruits of human creativity and innovation.
- Examples of (IP) include :

✓ Inventions

✓ Works of art

✓ Designs

✓ Brands

✓ Computer programs

Computer science

❖ **Electronic Intrusion**

- is unauthorized access to networks and information systems or any other type of information attack.
- electronic intrusion includes activities to steal or corrupt sensitive information, destroy software, disable an information system, steal service, and other types of information system attacks such as spoofing

Computer science

- **Types of Electronic Intrusion**

1. **Phishing:** involves tricking people into revealing sensitive information such as usernames
2. **Malware:** Using software, such as viruses to damage or control a computer system
3. **Password attacks:** that aim to gain unauthorized access to networks, or online accounts by cracking password.
4. **Personal devices**
5. **Data**

Computer science

- **The most common security risks of computer:**

1. Viruses
2. Spyware
3. Adware
4. General mistakes
5. Internet and network attack
6. System failure

❖ Malware

- Short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems.
- Examples of common malware include viruses, worms, Trojan Horse, spyware, adware.

Computer science

❖ Viruses

- are small programs that can copy itself and infect a computer without the permission or knowledge of the user .
- The first computer virus was called Creeper.

➢ Characteristics of computer viruses

1. The ability to replicate itself
2. Connecting itself to another program called the host.
3. They can spread from one computer to another

Computer science

❑ Types of Viruses

1. Worms : this is a computer program that replicates itself a swift pace. It spreads only across Internet networks.
2. Macro virus : is associated with application software like word and excel and other data files.
3. Trojan horse : It does not replicate itself to other computers like virus and worms. It is a hidden piece of code which steal the important information of user.

Computer science

❖ Protection from virus

- Computer Viruses are very harmful to computer system. they can destroy data and information.
- So, computer should be protected from viruses

✓ The computer system can be protected from the viruses by the following ways :

1. Install anti-virus software from a well known reputed company and use it regularly, and use firewall.

Computer science

2. Lock the computer system using password to prevent your computer from being used by others.
3. Do not download any program from the internet unless you are confirmed that they are virus free.
4. Be careful with checking mail having attached document.
5. Use strong passwords and two-factor authentication.
6. Keep software and security systems up to date