1. **computer security**

the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment—namely, serial numbers, doors and locks, and alarms. The protection of information and system access, on the other hand, is achieved through other tactics, some of them quite complex.

2. Importance of Computer Security

If a computer security system is not put in place until a problem arises, it could lead to major issues and concerns, and it will be too late to resolve them. Especially in a data-driven world, it is imperative to keep all kinds of information from malicious hackers and prevent vital information from falling into the wrong hands for misuse.

Computer security helps keep valuable information protected and maintain the health of a computer with no disruptive behavior in its performance caused by viruses and malware.

That's all for the importance and need of computer security. Read on to learn about different categories of computer security.

3. Components of computer system

The components of a computer system that needs to be protected are:

Hardware, the physical part of the computer, like the system memory and disk drive

Firmware, permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user

Software, the programming that offers services, like operating system, word processor, internet browser to the user

4. Types of Computer Security

Here are a few types of computer security tactics that are used widely for the protection of software, hardware, electronic data, and network in computer systems.

Application Security

Application security is the introduction of security features in applications during their development process. This actively helps prevent potential cyber threats such as data breaches, denial-of-service attacks (DoS), SQL injection, and many others. Some examples of application security tools are antivirus software, firewalls, web application firewalls, encryption, etc.

Information Security

Information security is a set of practices that aim to protect the confidentiality, integrity, and availability (known as the CIA triad) of data from unauthorized access and misuse.

Network Security

Network security is any activity that aims to protect the integrity and usability of a network and data. It consists of both hardware and software technologies that are specifically designed to prevent unauthorized intrusion into computer systems and networks.

Endpoint Security

End-users are increasingly becoming the biggest security risk unintentionally. With no-fault from their end, exempting the lack of awareness, the virtual gates of an organization are open to hackers and attacks. Most of the end-users are unaware of the ICT policy, and therefore, it is imperative that the users who handle sensitive information on a regular basis understand and be knowledgeable about all comprehensive security policies, protocols, and procedures.

Internet Security

Internet security is one of the most important types of computer security that come with a set of rules and protocols that focus on specific threats and activities that happen online. It provides protection against hacking, DoS attacks, computer viruses, and malware.

5. Why Do Users Get Attacked?

Before getting into how to secure data from breaches, we must try to understand the motives behind these attacks. By knowing the motives behind the attacks, it's easy for cyber security professionals to secure the systems. The main motives for attacking an organization's or individual's computer are：

Disrupting a business' continuity: If a business is disrupted, it causes great harm to the organization in the form of lost profits, fraud, and damage to its reputation.

Information theft and manipulating data: Hackers take confidential information that they steal from organizations and sell it to individuals or groups on the black market.

Creating chaos and fear by disrupting critical infrastructure: Cyber terrorists attack a company or a government body to disrupt their services, doing damage that can potentially affect an entire nation.

Financial loss to the target: Hackers attack an organization or business and disrupt their services in such a way that the target has to allocate substantial funds to repair the damage.

Achieving a state's military objectives: Rival nations continuously keep an eye on each other and sometimes employ cybercriminal tactics to steal military secrets .

Damaging the reputation of target: The hacker may have personal reasons to attack an organization or individual so that their reputation suffers.

Propagating religious or political beliefs: Hackers may infiltrate websites to promote religious dogma or a certain political agenda, usually to sway voters to vote a certain way.

6. Healthy Computer Security Principles and Practices

Since attacks on computer systems and networks are becoming relentlessly inventive day by day, the need for combating them is vital. Listed are a few of the healthy computer security practices that one must be aware of to safeguard against growing computer threats.

- **Ensure physical computer security:**
    - **Install security and anti-virus software**
    - **Activate firewall**
- **Update your software and stay alert on news and the latest software**
- **Do not click on email attachments from unknown senders**

- **Make your passwords strong and change them regularly**
- **Ignore pop-ups and drive-by downloads when using the Internet**
- **Educate yourself on the fundamentals of computer security and the latest cyber threats**
- **Perform regular scans and create system backups periodically**