CYBER SECURITY

Cyber security is the practice of protecting critical systems, sensitive information, networks, and programs from digital attacks. It is also called computer security or information technology security. In other words, cyber security is the protection of computer systems and networks from information disclosure, or damage to their hardware, software, or electronic data, and from the disruption or misdirection of the services they provide.

In this era of information technology, cyber security is a widely known and most important topic.

Common cyber threats :

Nowadays because of work from home, increased the use of internet in day-to-day life, and newly added cloud services the threats of cyber security are increased on large scale. Some of the common threats are as follows:

1. **Malware-** Malicious software (Malware) installed on a computer can leak personal information and give control of the system to the attacker and delete data permanently

2. **Side-channel attack-** This attack (SCA) mainly aims at extracting secrets from a chip or a system, through measurement and analysis of physical parameters

3. **Ransomware -** Ransomware attacks work by gaining access to your computer or device, and then locking and encrypting the data stored on it.

4. **Phishing / social engineering-** In these attacks, attackers Manipulate the user or take the help of their weakness to gain personal information and access it.

5. **Insider threats -** the threat that an insider will use his or her authorized access, wittingly or unwittingly, to harm the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems.

6. **Distributed denial-of-service (DDOS) attacks -** A DDOS attack involves multiple connected online devices, collectively known as a botnet, which are

used to overwhelm a target website with fake traffic.

7. Advanced persistent threats (apts) – In this attack, an unauthorized user gets access to your system or network.

This mainly includes Hacking and stealing important data

8.Man-in-the-middle attacks - In these attacks cybercriminals are directly involved in the crime. He intercepts and relays messages between two parties to steal data. For example, on an unsecured Wi-Fi network,

9.Reverse engineering – with the help of reverse engineering, the software is deconstructed to reveal its designs, code, architecture, or extract knowledge from the object.

10.Spoofing – In this attack fraudsters pretend to be someone or something else to win a person's trust and get information.

The system at risk :

As the use of computers and the internet increases, we store personal, business-related, and government information on computers and sometimes on a cloud. Which leads to an increase in the systems at risk. Some systems which can face cyber attacks are as follows:

Financial systems, Utilities and industrial equipment, Aviation , Consumer devices, Large corporation, Automobiles, Government, Internet of things, Medical system, Energy sector

System Protection :

System protection techniques help to reduce cyber threats, vulnerability, attacks by preventing or eliminating them or minimizing the harm caused by cyber-attacks. Some common techniques of system protection are as follows:

•Security by design- Security by design is an approach to software and hardware development that makes the system free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards, and adherence to best programming practices.

•Security architecture- it is a set of security principles, methods, and models designed to align with your objectives and help keep your organization safe from cyber threats.

•Security measures - The system can be protected by applying appropriate security measures like setting up a strong password, Setting up a firewall, installing antivirus, Using Two-Factor or Multi-Factor Authentication

•Secure coding - In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities

•Secure operating systems - we can reduce the chances of a cyber attack by using a trusted operating system that supports multilevel security systems.

•End-user security training- Most cyberattack in the last few years is due to users mistakes, A common mistake that users make is saving their user id/password in their browsers to make it easier to log in to banking sites. This is a gift to attackers who have obtained access to a machine by some means. These mistakes can be avoided by providing awareness training to users.

•Digital hygiene – Digital hygiene is much familiar with personal hygiene. As we take personal care to stay healthy, we should take care of our Computers or Digital data by updating, taking Backup regularly, installing anti-virus, and keeping the hard drive clean.

Looking at the speed of technology development in the next 10 years we will use additional authentication methods and technologies to protect our system and we can not deny the role of artificial intelligence in future cyber security.