CYBER SECURITY

➔ **Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

➔ A successful cyber security approach has multiple layers of protection spread across the computers, networks, programs or data that one intends to keep safe. In an organisation,the people,processes,and technology must all complement one another to create an effective defence from cyber attacks.

➔ The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories

☐ **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

☐ **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

☐ **Information security** protects the integrity and privacy of data, both in storage and in transit.

☐ **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- ☐ **End-user education** addresses the most unpredictable cyber-security factor: *people*. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

➔ **Cyberattack** is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices.

➔ **Scale of the cyber threat-**

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

➔ **Types of Cyber Threats:-**

- ☐ **Malware** means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. The different types of Malware include:virus,spyware,ransomware,adware,etc.
- ☐ **Phishing** is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.
- ☐ **Social engineering** is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.
- ☐ A **denial-of-service attack** is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.
- ☐ **End-user protection** or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

➔ Cyber safety tips - protect yourself against cyberattacks

Then how to protect yourself from these threats...here are a few steps to follow:

1. **Update your software and operating system:**This means you benefit from the latest security patches.
2. **Use anti-virus software:**Security solutions like Kaspersky Total Security will detect and remove threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:**Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:**These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:**This is a common way that malware is spread.
6. **Avoid using unsecured WiFi networks in public places:**Unsecure networks leave you vulnerable to man-in-the-middle attacks.