CYBERSECURITY

-Uttara Ketkar

What is meant by cybersecurity?

- Cyber security refers to the practice of protecting computer systems and networks from attack, damage, or unauthorized access via certain technologies, processes, and practices.

What is a vulnerability?

- Vulnerability is a flaw in the security system of a network which can be potentially exploited by a cyber-attacker to gain unauthorized access and perform actions that compromise the security of the system.

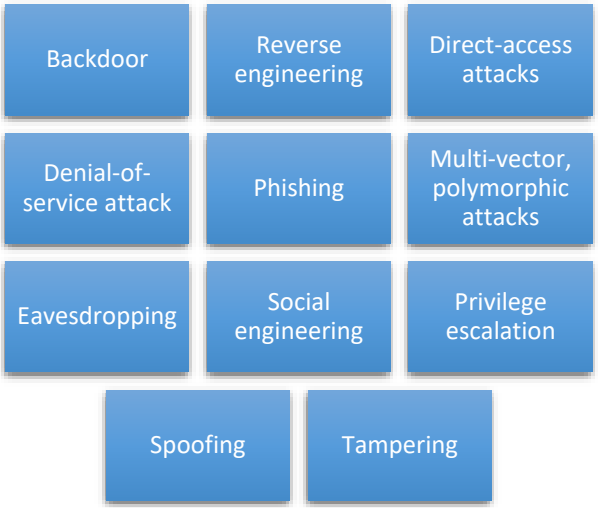

Fig 1: Types of threats

What is a malware?

- Malware – a malicious software typically consisting of code developed by cyber attackers, designed to cause extensive damage to data and system of the computer user.

Types of Malware:

- **Computer virus:** When executed, replicates itself by modifying other computer programs and inserting its own code.
- **Computer worm:** Virus writes its own code into the host program, causing infection and damage.
- **Trojan horse:** Any malware which misleads users of its true intent.

- **Ransomware:** Malware that threatens to publish the victim's data or block access to it unless a ransom is paid.
- **Spyware:** Aims to gather info about an organization, without their knowledge, and send info to hack another entity without the consumer's consent.
- **Adware:** Presents unwanted advertisements to the user of a computer - a pop-up or sometimes in an "unclosable window".
- **Rogue security:** Misleads users that there is a virus on their computer and aims to convince them to pay for a fake malware removal tool.
- **Scareware:** Tricks users into believing their computer is infected with a virus, then suggests to download and pay for fake antivirus software.

Elements of cybersecurity:

- **Network Security:**
    1. Network security ensures internal protection by keeping close surveillance on passwords, firewalls, internet access and more.
    2. The main focus is to protect internal information by monitoring employee behaviour and network access.
- **Application Security:**
    1. Application security is the general practice of adding features or functionality to software to prevent a range of different threats.
    2. These include denial of service attacks and other cyberattacks, and data theft situations.
- **Endpoint Security:**
    1. Endpoint security refers to a method of protecting the corporate network when accessed via remote devices such as laptops or other devices.
    2. Each device with a remote connecting to the network creates a potential entry point for security threats.
- **Disaster recovery:**
    1. Disaster recovery plans aim at quickly redirecting available resources into restoring data and information systems following a disaster.
    2. A disaster can be classified as a sudden event that creates wide scoping, detrimental damage.
- **Database security:**
    1. Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability.
- **Data security:**
    1. Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle.
    2. It includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

Cybersecurity incident response plan:

i. **Preparation:** Preparing stakeholders on the procedures for handling computer security incidents or compromises.
ii. **Detection and analysis:** Identifying and investigating suspicious activity to confirm a security incident, prioritizing the response based on impact and coordinating notification of the incident.
iii. **Eradication & Recovery:** Isolating affected systems so as to prevent escalation and limit impact, looking on the genesis of the incident, eliminating malware, and restoring systems and data when a threat no longer remains.
iv. **Post Incident Activity:** Inferences and observations of the incident, its cause and the organization's response with the aim of improving the incident response plan and future response planning.

Career options in cybersecurity:

1. **Security analyst**
   Analyses and assesses vulnerabilities in the company's digital assets, investigates using available tools and takes measures to eradicate the detected vulnerabilities and recommends solutions and best practices.
2. **Security engineer**
   Performs security monitoring, data analysis, and forensic analysis, to detect security incidents, and works on the incident response.
   He/she implements secure network solutions in the defence of any cyber attacker.
3. **Security architect**
   Designs a security system or major components of a security system, and may head a security design team building a new security system.
   Ensures that the networks confidentiality and integrity is maintained.
4. **Security administrator**
   Installs and manages organization-wide security systems.

He/she performs vulnerability tests and monitors network traffic for suspicious behaviour.

To conclude:

In today's world where almost every sector of human interaction involves the use of computer systems, cybercrime is the biggest challenge! With technological advancements and increased access to data, cybersecurity has become the need of the hour. It is our shared responsibility to keep ourselves aware of the threats and keep our systems updated!