Malware

Malware is intrusive software designed by cybercriminals to steal data or harm systems (Cisco).

Types of malware

Adware	Displays unwanted advertisements on your screen.
Spyware	Observes your computer activity and reports it to the attacker.
Viruses	Infects files or system areas and spreads by self-replicating
Worms	Spreads by self-replicating without user action.
Trojans	Masquerades as legitimate software while executing malicious actions.
Ransomware	Encrypts systems and data, demanding ransom for decryption
Rootkit	Gains admin access and is difficult to remove.
Keyloggers	Programs that log keystrokes.
Malicious crypto miners	Uses your computer to mine cryptocurrency for attackers

Malware Detection & Prevention

First Step if Infected:

> Disconnect from the network immediately.

Detection/Removal Tools

> Anti-malware, endpoint security, network monitoring, Antivirus software (updated regularly).

Prevention Tips

- Keep OS/apps patched and updated.
- Verify email senders before opening attachments.
- Avoid suspicious downloads and links.
- Disable macros in Office documents (unless needed).
- Use antivirus, firewalls, and email filters.
- Beware of social engineering attempts.

How Malware Spreads

1) Opening a malicious email attachment.
2) Visiting unsafe websites.
3) Downloading files from untrusted sources.
4) Clicking malicious links in messages (e.g., WhatsApp, Facebook).
5) Using unknown USBs, SD cards, or CDs

***Key Reminder** : Never use USB memory sticks that you may have found in common areas. They may have been planted there intentionally for you to find with the hope you would insert them into your computer*

Zero-day Attacks

A zero-day attack exploits an unknown hardware, firmware, or software vulnerability with no available immediate fix.
Life Cycle: Vulnerability found → exploit created → attack occurs → vendor discovers → patch released.

***Key Note:** Users usually cannot stop zero-day attacks directly. Only way to prevent it is wareness + safe practices (patching, avoiding phishing, careful downloads) reduce risk.*

Viruses

According to CISA, a virus infects files or system areas and self-replicates

Virus Symptoms

Slow performance	Corrupted or missing files	Pop-up and adware
Program and operating crash	Spinning hard drive	System malfunctions

***Effects:** Stolen personal information i.e. Identity theft & Lost account access*

Ransomware

Malware that encrypts files, making them and related systems unusable.
Ransomware encrypts files, demanding payment for decryption. It's a major threat to all industries, often spread through phishing emails with malicious attachments.

Denial-of-Service (Dos) Attacks

A Denial-of-Service (DoS) attack disrupts systems, devices, or networks by overwhelming them with traffic, preventing legitimate access. This can halt business operations, affect services like email, websites, and messaging, and result in financial loss. Attackers may be motivated by financial gain, hacktivism, or system access attempts

Distributed DoS (DDos)

A Distributed Denial-of-Service (DDoS) attack occurs when multiple hijacked devices overwhelm a target system. Attackers exploit vulnerabilities to control these devices and direct them to flood the host with traffic

Advance persistent threat

An Advanced Persistent Threat (APT) is a long-term, stealthy attack on networks by nation-states, state-sponsored groups, or organized crime, aiming for intelligence, military, or financial gains.

Protection

1. Use Multi-Factor Authentication (MFA).
2. Never share credentials.
3. Report suspicious activity (e.g., mouse moving by itself, odd files appearing).
4. Cyber teams monitor for unusual patterns, but users are often first line of defense.

Signs of a DoS/DDoS Attack:

Slow network performance	Inaccessible websites
Inaccessible servers	Failed authentication attempts

Avoiding DDoS/DoS Attacks

1) Use antivirus software on personal devices.
2) Enable a firewall for protection.
3) Secure your devices vulnerabilities on hardware/ software