What is Malware?

Malware, short for "malicious software," refers to harmful programs such as viruses, worms, spyware, ransomware, adware, and trojans. These programs are designed to infiltrate, damage, or steal information from devices and networks.

How Does Malware Get Downloaded?

Cybercriminals use various methods to distribute malware, including:

1. Man-in-the-Middle (MitM) Attacks

Attackers intercept communication between two parties, hijacking the session between a client and host.

2. Phishing Attacks

Social engineering techniques are used where attackers pose as trusted contacts to deceive users into downloading malicious software or sharing sensitive information.

Protecting Against Malware

1. Reduce Device Vulnerability

- Keep your software and operating systems updated.
- Use a Virtual Private Network (VPN) when accessing the internet.
- Only download apps and programs from trusted sources (e.g., official app stores).
- Install and regularly update antivirus software.
- Avoid using public Wi-Fi for sensitive activities.

2. Be Vigilant Online

- Visit only secure and reputable websites.
- Do not open attachments or files from unknown sources.
- Avoid clicking on suspicious pop-ups and links.

How to Tell If Your Device is Infected with Malware

Signs that your device may be infected include:

- Slow performance
- Frequent or unusual pop-ups
- Unexpected software installations
- Browser redirects to unfamiliar websites
- Disabled security features
- Excessive data usage
- Mysterious charges on accounts
- Device overheating
- Unauthorized access to accounts or files
- Missing or encrypted files

What to Do If Your Device Is Infected

If you suspect malware on your device, take the following steps:

1. **Disconnect from the Internet** – Prevent further data theft or malware spread.
2. **Run an Antivirus Scan** – Use security software to detect and remove malware.
3. **Enter Safe Mode (if necessary)** – This can prevent malware from running while you remove it.
4. **Check for Suspicious Programs and Processes** – Identify and uninstall any unfamiliar software.
5. **Remove Malware Manually (if needed)** – If antivirus software fails, manually delete harmful files.
6. **Restore Your System (if necessary)** – Consider restoring your device to a previous state.
7. **Change Your Passwords** – Secure your accounts in case of unauthorized access.
8. **Monitor for Identity Theft or Further Issues** – Watch for suspicious activity on your accounts.
9. **Seek Professional Help (if necessary)** – If issues persist, consult an expert or reinstall your operating system.

Need More Help?

For more information, contact Cyber-Seniors at **844-217-3057** or visit **www.cyberseniors.org**.

*This lesson guide was made possible by a **CIRA Net Good Grant**. Learn more at **cira.ca**.*