Digital Security- : Understanding Viruses, Malware, and Phishing

Introduction to Digital Threats

The digital world offers many benefits but also poses risks

Three major threats:

Understanding these threats is crucial for online safety

viruses,

Malware

phishing

What is a Computer Virus?

Definition: A computer virus is a type of malicious software

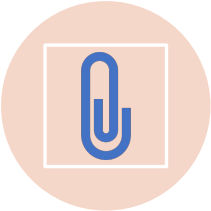
It replicates and spreads by attaching to other programs

Viruses can corrupt files, steal data, or damage system performance

They often require user action to spread (e.g., opening an infected file)

Types of Computer Viruses

Boot sector viruses: Infect the master boot record



File infectors: Attach to executable files

Macro viruses: Embed in document files (e.g., Word, Excel)

Polymorphic viruses: Change their code to avoid detection

Signs of a Virus Infection

- Slow computer performance
- Unexpected pop-up windows
- Programs crashing frequently
- Files disappearing or becoming corrupted
- Strange hard drive activity

Introduction to Malware

Malware = Malicious Software

Broader category that includes viruses and other threats

Designed to exploit, damage, or gain unauthorized access to systems

Can be more sophisticated and harder to detect than viruses

Types of Malware

- Trojans: Disguised as legitimate software
- Worms: Self-replicating and spread without user action
- Ransomware: Encrypts files and demands payment for decryption
- Spyware: Secretly monitors user activity
- Adware: Displays unwanted advertisements

How Malware Spreads

- Email attachments
- Infected websites
- Software downloads from unreliable sources
- Peer-to-peer file sharing
- Exploiting software vulnerabilities

Consequences of Malware Infections

- Data theft (personal information, financial data)
- System damage or slowdown
- Financial losses (e.g., ransomware payments)
- Privacy breaches
- Identity theft

What is Phishing?

Definition: A cyber attack that uses disguised email as a weapon

Goal: Trick the recipient into believing the message is genuine

Aims to steal sensitive information or install malware

Often impersonates trusted entities (banks, social media, etc.)

Types of Phishing Attacks

Spear phishing: Targeted attacks on specific individuals

Whaling: Targeting high-profile individuals (e.g., CEOs)

Smishing: Phishing via SMS text messages

Vishing: Voice phishing over phone calls

Clone phishing: Replicating legitimate emails with malicious content

Common Phishing Techniques

1. Creating a sense of urgency
2. Using official-looking logos and email formats
3. Exploiting current events or crises
4. Offering too-good-to-b e-true deals
5. Requesting sensitive information via email

Red Flags in Phishing Emails

- Misspellings and grammatical errors
- Generic greetings (e.g., "Dear Sir/Madam")
- Suspicious sender email addresses
- Requests for personal information
- Unexpected attachments or links

Protecting Against Viruses

Install and regularly update antivirus software

Keep your operating system and applications up to date

Be cautious when opening email attachments

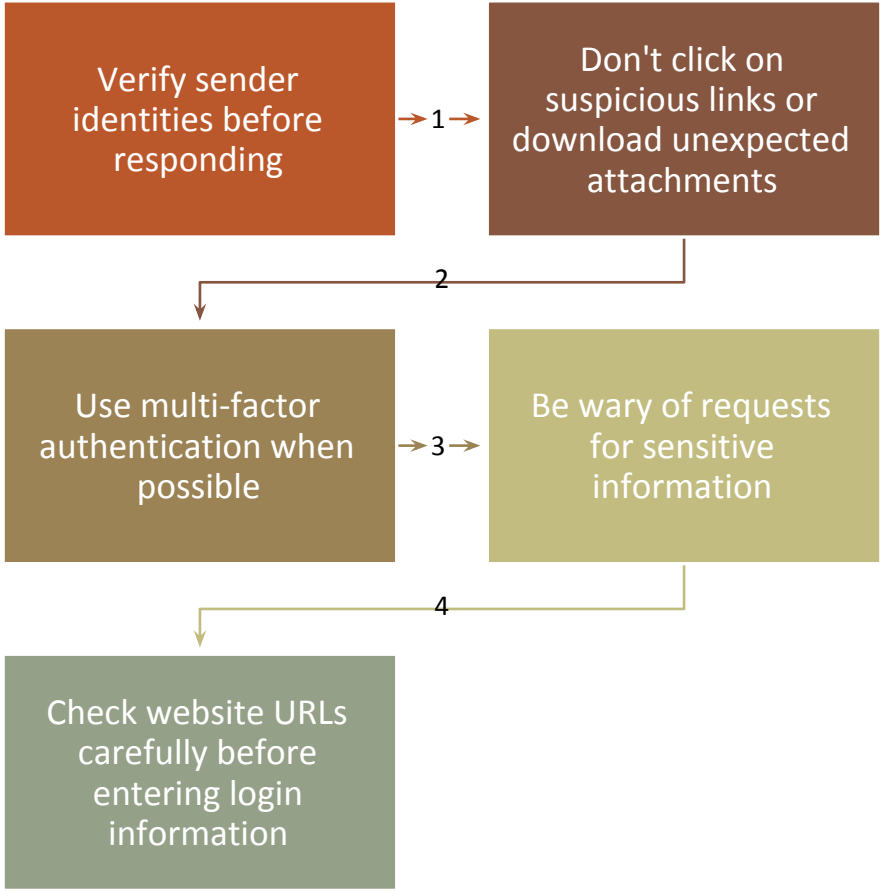
Avoid downloading files from untrusted sources

Regular system scans and backups

Defending Against Malware

- Use a comprehensive security suite
- Enable firewalls on your network and devices
- Practice safe browsing habits
- Be cautious with software downloads
- Keep all software patched and updated

Avoiding Phishing Attacks



General Cybersecurity Best Practices

- Use strong, unique passwords for each account
- Implement multi-factor authentication
- Regularly back up important data
- Educate yourself about current cyber threats
- Be skeptical of unsolicited communications

What to Do If You're Compromised

DISCONNECT FROM THE INTERNET IMMEDIATELY

RUN A FULL SYSTEM SCAN WITH UPDATED ANTIVIRUS SOFTWARE

CHANGE PASSWORDS FOR ALL ACCOUNTS (FROM A CLEAN DEVICE)

MONITOR FINANCIAL STATEMENTS AND CREDIT REPORTS

REPORT THE INCIDENT TO RELEVANT AUTHORITIES IF NECESSARY

The Future of Digital Threats

Evolving threat landscape (AI-powered attacks, IoT vulnerabilities)

Importance of staying informed about new threats

Emerging technologies in cybersecurity (AI defense, blockchain)

The role of user education in cybersecurity