Unsafe Hardware

Threat actors embed vulnerabilities directly into hardware and accessories.

How to spot it:
- Too-good-to-be-true deals

Social Engineering

Scammer manipulates people by pretending to be a legal entity or other authoritative body to steal their sensitive personal or financial information (a.k.a. "phishing"). The malicious code is sent via links or attachments to emails, direct messages and texts.

How to spot it:
- New files or network connections on your system that you did not add
- Unsolicited requests for configuration information
- Odd sender email address, phrasing, spelling

USB Malware Attack

Criminal uses removable storage devices, like USB drives, portable hard drives, smartphones, music players, SD cards, and optical media (CDs, DVDs, Blu-Ray) to infect computers or networks.

How to spot it:
- Unexpected access to files or newly created files on the device
- "Your connection is not secure"

Trusted Relationship

A hacker breaches a trusted third party, like a doctor's office, and uses their reputation to exploit patients.

How to spot it:
- Unusual logon behavior

How to stay cybersafe:

**DOs**

- Use multi-factor authentication and strong, unique passwords across all of your accounts.
- Be alert and skeptical. Learn to recognize scammer tactics.
- Be vocal. Report attacks to IT and notify coworkers, family, and friends.
- Keep software up-to-date.

**DON'Ts**

- Don't click on any links embedded in unsolicited emails or direct messages.
- Don't ignore browser warnings, e.g., "Your Connection is Not Secure" or "Your connection is not private".
- Don't get lazy. Follow all security protocols consistently.
- Don't trust any unsolicited emails or direct messages with promises of financial gain or urgent action.
- Don't trust any unsolicited emails or direct messages that ask for personal information.

TIP:
- Government agencies (IRS, etc.) will reach out via USPS first.