Cybersecurity: Understanding malware

Protect yourself online by understanding common threats.

What is it?

Malicious software, also known as malware, and viruses are the most common cyberattacks. Learning how to identify these attacks can help you prevent an infection on your computer, tablet, or cell phone.

Types of malware

Malware comes in a range of types. While this is not a complete list of threats, these are the most common malware attacks:

- **Viruses** replicate themselves to modify computer programs after they are activated by the user.
- **Worms** are another self-replicating attack that can spread across systems on their own.
- **Adware** is designed to flood your device with unwanted ads.
- **Spyware** secretly observes your device activities and reports it to the attacker.
- **Trojan**, also known as a Trojan horse, gives attackers access to your device to steal personal or financial information.
- **Ransomware** locks you out of your device until a ransom is paid.
- **Keyloggers** track key strokes so attackers can gain access to usernames, passwords, or financial information.

How can I prevent malware attacks?

Phishing scams

Malware is often delivered through phishing attacks, which come in as an email, text message, or phone call.

Phishing scams are often “spoofed” to look like they are coming from a known and trusted organization, like a bank or government office. They generally make unusual requests, such as asking you to pay a fine with a gift card.

Often, phishing scams try to create a sense of urgency by making time-bound claims. A common example is claiming that your account or personal information will be lost if you do not take immediate action.

Phishing emails and texts usually include attachments or links that may install malware on your computer when opened. Avoid opening links on attachments unless you are confident you know the sender. If you are unsure whether an email is real, search for the sender’s contact information and call them to confirm whether they sent it.

You can also hover your cursor over the name of the sender to verify the sender’s email address. If the name shows something different than what is listed in the sender field, you are likely dealing with a phishing email.

You can also hover your cursor over a link to see the destination URL. This will often appear as a small line of text in the lower left-hand side of your internet browser. Do not click any links that point to a different website than what the text suggests or that appear to be alpha-numeric codes.

If you receive a phishing email, delete it without taking any of the actions suggested.

Learn more about other common text scams.

Ransomware

Ransomware is a kind of malware that uses encryption to hold your data and information hostage until a ransom is paid to the attacker. It is downloaded to a device without your consent through malicious links, emails, texts, or websites.

Do not pay the ransom if your device is infected. It does not guarantee that your information will be released to you or that the ransomware will be removed from the device. Contact a local computer repair service for removal support.

You can help prevent ransomware by following the same tips provided in the phishing email section above and by installing a high-quality antimalware software. When in doubt about the legitimacy of an email or text, simply delete it without taking any of the actions requested in the message.