THE MANY FACES OF MALWARE

Malware is the combination of two words: "malicious" and "software." Cyberattackers use malware for many different purposes—all of them bad. Several activities can expose you to malware, including:

- Viewing and downloading infected email attachments
- Visiting compromised websites
- Downloading infected files from a cloud storage service like Office 365 or Google Drive
- Interacting with malicious ads and pop-up windows
- Downloading malicious applications, pirated content, or cracked software

Below are some of the different types of malware that cybercriminals use to try to gain access to devices, data, and systems. You are a critical line of defense against cyberattacks—so be sure to stay security conscious!

KEYLOGGER

Keyloggers record the keystrokes made on infected devices. They can capture passwords, account numbers, and other confidential data. Some can also copy screen captures, download logs, and web browsing histories.

BACKDOOR MALWARE

A malware backdoor is like an invisible backdoor to your home—a covert entrance criminals can use to come and go as they please on a device or network, without triggering any alarms or security.

MALVERTISING

Malvertising is "malicious advertising." More specifically, it's the use of malicious code within online ads.

Attackers hide dangerous code in online ads and try to trick you into visiting an unsafe website or downloading malware. You could encounter malvertising anywhere online—even on trustworthy websites.

POINT-OF-SALE MALWARE

Cybercriminals infect payment terminals with point-of-sale (POS) malware to steal credit card information during retail transactions. POS malware can gather credit card numbers, security codes, or even full magnetic strip data.

REMOTE ACCESS TROJAN

A remote access Trojan (RAT) is like Greece's legendary Trojan Horse: it comes disguised as something else, and you are tricked into letting it through your defenses.

RATs give attackers remote access to infected devices. They can act as an administrator from anywhere and use this access to spy on you, install additional malware, or steal sensitive information.

Want to learn more about these types of malicious software?

Watch our Malware Minute videos!

ADVANCED PERSISTENT THREAT

An advanced persistent threat (APT) is a prolonged, customized attack on a precise target. APTs are often the work of nation-state actors, who execute state-sponsored attacks on another nation's government agencies, critical infrastructure sector, and/or private industry.

APTs use customized malware and sophisticated social engineering to infiltrate their targets. APT malware is difficult to detect and remove, so attackers can remain in a system for a long time. These well-funded, efficient, and effective attacks can be extremely damaging.