What Is Malware?

Malware refers to any software designed to have a malicious purpose once deployed on a computer or network. Malware infection typically occurs without a user's knowledge and can affect both desktop and mobile devices. It can serve various purposes, from stealing information to spying on keystrokes and mining cryptocurrency using computer hardware.

Examples of Malware Infection Methods

01 PHISHING

The most common malware delivery system used by cyber criminals is via phishing messages. A file may be included as an attachment in the message itself or delivered via a web link that directs the recipient to download the file from an online storage location.

02 USB DRIVE

Cyber criminals will often drop USB thumb drives containing files that use enticing names to convince whoever finds it to plug the drive into their computer. Once this is done, the malware can easily infect the computer.

03 WEBSITES

Whether via social networking sites or a compromised legitimate site, websites can also deliver malware to an unsuspecting visitor. Because the files may be transferred through trustworthy means, many victims don't give these actions a second thought.

04 INFECTED FILES

Legitimate files and software may be infected with a virus. Once opened, they will operate as expected and install malware on the device in the background, usually without the user's knowledge or permission.

05 NETWORK

This type of malware can spread to other devices connected on the same network in addition to its primary target. Once installed via one of the other methods explained here, this malware will look for other connected devices to infect.

Who Could Be a Malware Target?

Any type of business, government, organization, or individual could be a malware target. Cyber criminals look to victimize anyone who isn't alert to the presence of malicious software. Due to many common tactics employed to trick users into trusting suspicious messages or files, detecting malware can be challenging.