What Is Malware and How to Defend Against It?

Malware is an abbreviated term meaning “malicious software.” This is software specifically designed to gain access to, disable, or damage a computer without the knowledge of the owner. Malware can steal sensitive information from your computer, erase data, gradually slow it down, or even send fake emails from your account without your knowledge. Malware is most commonly spread by opening or downloading a file containing malware, by clicking on links, or visiting a website that hosts harmful content.

Here are some common classes of malware:

Viruses: Viruses earn their name due to their ability to “infect” clean files on a computer. They can spread uncontrollably, damaging a computer’s functionality and corrupting, or deleting files.

Trojans: This kind of malware disguises itself as legitimate software, or is included in legitimate software that has been tampered with. It can act discretely and often creates a backdoor in your security to let other malware in.

Spyware: Spyware is malware designed to spy on you. It collects data such as keystrokes, browsing history, credit card numbers, and login information.

Worms: Ransomware infects your computer, encrypting your files or locking down your computer completely until a ransom is paid. If you refuse to pay, your computer remains locked, or your data is deleted.

Ransomware: Worms infect one computer and then use that computer’s network to spread to other machines. By exploiting network vulnerabilities, worms can send out thousands of copies of themselves in hopes of infecting new systems.

Adware: Although not necessarily malicious in nature, adware automatically delivers advertisements to host computers. It may use tracking tools to learn about your location and browsing history, using that information to serve up targeted ads to your screen. Adware often comes packaged with free games and software downloaded from the internet.

Follow these tips to help protect yourself from malware:

Keep your computer and software updated. These updates often include fixes that can improve the security of your system and help prevent malware attacks.

Purchase security/antivirus software. This type of software allows you to scan your computer for malware. You should run regular scans of your computer to catch malware early and prevent it from spreading. If you need to download something, you should use this program to scan that download for malware before opening it.

Be mindful of what you click on. Many websites that host harmful content will use banners and pop up advertisements, pretending to be an error message, or offering you a prize. When you visit these sites, harmful content is downloaded to your computer.

Be aware of what you are downloading. Downloads are one of the main ways people get malware, so remember to think twice about what you are downloading, and where you are downloading it from. Be cautious of websites that claim to offer free games and software. Search for reviews or information about that website before downloading or installing anything.

Be careful about opening email attachments or images. Do not open attachments or images in an email that you receive from a random person. It may contain harmful malware. You should also be cautious of suspicious looking emails you receive from friends. Some malware threats have the ability to automatically send copies from that user’s contact list. It may look like your friend is sending you a file, but it may actually be malware.

By following these tips, you can help protect yourself from a malware attack. Although no form of protection is absolute, a combination of personal awareness and protective tools will make your computer as safe as it can be.