FORTRA

Co-sponsored by Microsoft

How to Protect Your Data from Malware Attacks

Malware is often discovered because of its symptoms, such as a suddenly slower computer, slower internet connection, disappearing files, ad pop-ups without a browser open, or, in extreme cases, a complete takeover of the machine. By that point, it's too late. The best kind of malware protection is prevention, implemented through the following best practices.

1

ONLY USE LEGITIMATE SOFTWARE

A typical delivery method for malware is via compromised versions of popular software tools. Only download and install software on company computers and servers based on a pre-approved list or through guidance from your IT team.

KEEP ALL SOFTWARE UP TO DATE

Security-related software, including your antivirus program, firewalls, and similar apps, must always be running the latest available version. Through updates, these and other software tools can close loopholes and minimize vulnerabilities that can potentially be exploited.

2

3

AVOID INAPPROPRIATE PERSONAL DEVICE USE

Be aware of your organization's policy related to using personal devices, especially regarding connecting them to work-sanctioned machines, networks, or systems. Malware can easily be transmitted to organizational hardware through a USB connection to a personal device.

INSPECT ALL INCOMING MESSAGES CAREFULLY

Make sure you examine and assess all incoming messages to your professional or personal inboxes with care. Pay particular attention to messages containing downloadable files or links to them, even if the sender seems legitimate.

4

5

BACK UP YOUR DATA REGULARLY

Ensure all your important data are backed up regularly using your organization's existing policy or procedure. It's also wise to back up your most crucial files in multiple physical or cloud-based storage locations.