NYC Digital Safety
Privacy & Security

Managing a Malware Attack

Learn how to identify, avoid, and deal with malware on different kinds of devices.

1. What Is Malware?

Malware stands for “malicious software,” and is a sort of umbrella term that covers different kinds of software that can infect, disrupt, and gain unauthorized access to a device.

Malware can infect computers, phones, and tablets. Here are a few forms of malware that you might have heard of before:

- **Ransomware:** Malware that can encrypt files and lock someone out of their device
- **Spyware:** Malware that gathers information about user
- **Adware:** Often takes the form of out-of-control pop-up ads
- **Worms:** A type of virus that actually copies itself and sends itself to other users
- **Virus:** A form of malware that can infect devices and corrupt data and software. Viruses operate by replicating themselves via code

What are some types of viruses?

- **Trojan virus:** A famous kind of computer virus that gets onto a machine by being disguised as a legitimate program. Users are tricked into installing or downloading something that contains a trojan virus
- **Browser hijacker:** Viruses that can infect a browser and change settings or redirect users to malicious sites
- **Macro virus:** Viruses that can infect macros in Microsoft Word
- **File infector virus:** A virus that can infect and spread among critical computer files

2. How Can You Tell if You Have Malware?

Malware isn’t alway easy to detect, unfortunately. However, there are some signs and things you can look for to determine whether or not you have malware on your device.

One thing you can do is install a security software that will scan your device for malware. However, do your research and be sure to download a legitimate tool! Some malware actually impersonates security software and tricks you into installing it.

Note that some security software might cost money. However, there are options for different price points, and many devices have security software installed, so you can decide what is the best option for you.

Here are some ways to help you identify potential malware:

- Your device is running very slowly or keeps crashing
- You can't shut down or restart your device
- You are missing files
- You get unexpected error messages
- You are seeing strange, mass emails sent from your account
- Your browser starts redirecting you or is lagging
- You keep getting pop-up windows or excessive and interfering ads
- Your battery drains quickly
- [For laptops] The fan runs continuously and loudly
- You're seeing apps, open tabs, and things you didn't open or install on your device

3. What Can You Do if You Have Malware?

If you suspect you've downloaded or your computer has been infected by malware, check to see if nefarious software is present and then proceed with removing it.

It is helpful to check and confirm your suspicions first, since some of the signs of malware can actually be signs of other issues. For example, a battery that drains quickly could just be a sign of an aging device!

But if you do find you have a larger issue, here's what to do:

- Stop doing things like online shopping or entering in passwords for accounts until you've resolved the problem. Change your passwords after you deal with the issue
- If your device is part of a network, disconnect it to prevent the malware from spreading
- Reboot your device in Safe Mode to better run your security software and deal with your malware infection
    - **Windows:** Press and hold F8 as soon as the reboot begins, and then choose Safe Mode from the menu. Then, run your security software scan
    - **Mac:** Hold down the Shift key while rebooting, and then perform your security software scan
- Make sure your security software is up-to-date
- If you don't have security software installed, install a reputable type of security software for your particular device. You can search for recommendations and lists from legitimate sources such as technology review sites and blogs like *The New York Times' Wirecutter* (https://www.nytimes.com/wirecutter/)
- Once you have your security software ready to go, run a scan on your device to see if malware is present
- Use your security software to help you remove it
- For more severe infections, you might need to reinstall your operating system. Visit your device manufacturer's official website for directions on how to do this
- If you still need help, contact tech support for your device (this might be covered by the warranty)
- Change your passwords and monitor your accounts for fraud after a malware infection

4. How Can You Avoid Malware?

Here are things you can do to protect your devices from malware:

- Be cautious when installing software, apps, and browser extensions. Malware can hide in these things, so be sure you are installing reputable and legitimate software on your device
- Keep your security settings up-to-date on your devices and your browsers. Install operating system updates, patches, and security updates in a timely manner.

- Be on the alert for phishing schemes and avoid clicking links or downloading files from suspicious or unknown sources
- Pay attention to the websites you are visiting and pay attention to warnings from your browser about unsecured sites
- Back up your data regularly to keep it protected and recoverable in case you end up with malware
- Install security software to monitor your device and help you block, detect, and remove malware

5. Make a Plan

Use this space to write down your plans and ideas for things you can do to avoid malware: