Malware

Malware includes viruses, spyware, and other unwanted software that gets installed on your computer or mobile device without your consent. These programs can cause your device to crash, and can be used to monitor and control your online activity. They also can make your computer vulnerable to viruses and deliver unwanted or inappropriate ads. Criminals use malware to steal personal information, send spam, and commit fraud.

- Avoid Malware
- Detect Malware
- Get Rid of Malware
- Report Malware

Avoid Malware

Scam artists try to trick people into clicking on links that will download viruses, spyware, and other unwanted software — often by bundling it with popular free downloads. To reduce your risk of downloading malware:

- **Install and update security software, and use a firewall.** Set your security software, internet browser, and operating system (like Windows or Mac OS X) to update automatically.
- **Don’t change your browser’s security settings.** You can minimize "drive-by" or bundled downloads if you keep your browser’s default security settings.
- **Pay attention to your browser’s security warnings.** Many browsers come with built-in security scanners that warn you before you visit an infected webpage or download a malicious file.
- **Instead of clicking on a link in an email, type the URL of a trusted site directly into your browser.** Criminals send emails that appear to be from companies you know and trust. The links may look legitimate, but clicking on them could download malware or send you to a scam site.
- **Don’t open attachments in emails unless you know who sent it and what it is.** Opening the wrong attachment — even if it seems to be from friends or family — can install malware on your computer.
- **Get well-known software directly from the source.** Sites that offer lots of different browsers, PDF readers, and other popular software for free are more likely to include malware.
- **Read each screen when installing new software**. If you don’t recognize a program, or are prompted to install additional “bundled” software, decline the additional program or exit the installation process.
- **Don’t click on popups or banner ads about your computer’s performance.** Scammers insert unwanted software into banner ads that look legitimate, especially ads about your computer’s health. Avoid clicking on these ads if you don’t know the source.
- **Scan USBs and other external devices before using them.** These devices can be infected with malware, especially if you use them in high traffic places, like photo printing stations or public computers.
- **Talk about safe computing.** Tell your friends and family that some online actions can put the computer at risk: clicking on pop-ups, downloading "free" games or programs, opening chain emails, or posting personal information.
- **Back up your data regularly**. Whether it's your taxes, photos, or other documents that are important to you, back up any data that you'd want to keep in case your computer crashes.

Detect Malware

Monitor your computer for unusual behavior. Your computer may be infected with malware if it:

- slows down, crashes, or displays repeated error messages
- won't shut down or restart
- serves a barrage of pop-ups
- serves inappropriate ads or ads that interfere with page content
- won’t let you remove unwanted software
- injects ads in places you typically wouldn’t see them, such as government websites
- displays web pages you didn't intend to visit, or sends emails you didn't write

Other warning signs of malware include:

- new and unexpected toolbars or icons in your browser or on your desktop
- unexpected changes in your browser, like using a new default search engine or displaying new tabs you didn’t open
- a sudden or repeated change in your computer's internet home page
- a laptop battery that drains more quickly than it should

Get Rid of Malware

If you suspect there is malware on your computer, take these steps:

- **Stop shopping, banking, and doing other online activities** that involve user names, passwords, or other sensitive information.
- **Update your security software**, and then scan your computer for viruses and spyware. Delete anything it identifies as a problem. You may have to restart your computer for the changes to take effect.
- **Check your browser** to see if it has tools to delete malware or reset the browser to its original settings.
- **If your computer is covered by a warranty** that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem.
- **Many companies — including some affiliated with retail stores — offer tech support.** Telephone and online help usually are less expensive, but online search results might not be the best way to find help. Tech support scammers pay to boost their ranking in search results so their websites and phone numbers appear above those of legitimate companies. If you want tech

support, look for a company’s contact information on their software package or on your receipt.

Report Malware

If you think your computer has malware, the Federal Trade Commission wants to know. File a complaint at www.ftc.gov/complaint.
Tagged with: computer security, cyber security, malware, personal information, privacy

November 2015