

## Malware

*Malware is short for "malicious software." It includes viruses and spyware that get installed on your computer, phone, 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. Criminals use malware to steal personal information, send spam, and commit fraud.*

### Avoid Malware

Scam artists try to trick people into clicking on links that will download malware and spyware to their computers, especially computers that don't use adequate security software. To reduce your risk of downloading unwanted malware and spyware:

- **Keep your security software updated.** At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically.
- **Don't click on any links or open any attachments in emails unless you know who sent it and what it is.** Clicking on links and opening attachments – even in emails that seem to be from friends or family – can install malware on your computer.
- **Download and install software only from websites you know and trust.** Downloading free games, file-sharing programs, and customized toolbars may sound appealing, but free software can come with malware.
- **Minimize "drive-by" downloads.** Make sure your browser security setting is high enough to detect unauthorized downloads. For Internet Explorer, for example, use the "medium" setting at a minimum.
- **Use a pop-up blocker and don't click on any links within pop-ups.** If you do, you may install malware on your computer. Close pop-up windows by clicking on the "X" in the title bar.
- **Resist buying software in response to unexpected pop-up messages or emails,** especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers use to spread malware.
- **Talk about safe computing.** Tell your kids 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 text files or photos 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 up a barrage of pop-ups
- 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
- new and unexpected icons in your shortcuts or on your desktop
- 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 is 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 run it to 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.
- 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 on the phone, online, at their store, and in your home. Decide which is most convenient for you. Telephone and online help generally are the least expensive, but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a repair person to come into your home.
- Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do differently to avoid it in the future.

## Report Malware

If you think your computer has malware, the Federal Trade Commission wants to know. File a complaint at

[www.ftc.gov/complaint](http://www.ftc.gov/complaint) (<http://www.ftc.gov/complaint>).

September 2011

## You Might Also Like

- [Understanding Mobile Apps](http://onguardonline.gov/articles/0018-understanding-mobile-apps) (<http://onguardonline.gov/articles/0018-understanding-mobile-apps>)
- [Common Online Scams](http://onguardonline.gov/articles/0002-common-online-scams) (<http://onguardonline.gov/articles/0002-common-online-scams>)
- [Spam](http://onguardonline.gov/articles/0038-spam) (<http://onguardonline.gov/articles/0038-spam>)