



MINIMIZING THE EFFECTS OF MALWARE

Malware is short for “malicious software;” it includes viruses — programs that copy themselves without your permission — and spyware, programs installed without your consent to monitor or control your computer activity. Criminals are hard at work thinking up creative ways to get malware on your computer. They create appealing web sites, desirable downloads, and compelling stories to lure you to links that will download malware, especially on computers that don’t use adequate security software. Then, they use the malware to steal personal information, send spam, and commit fraud.

It doesn’t have to be that way. OnGuardOnline.gov says consumers can minimize the havoc malware can wreak, and reclaim their computers and their electronic information.

Computers may be infected with malware if they:

- slow down, malfunction, or display repeated error messages
- won’t shut down or restart
- serve up a lot of pop-up ads, or display them when you’re not surfing the web
- display web pages or programs you didn’t intend to use, or send emails you didn’t write.

If you suspect malware is on your computer...

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. Malware on your computer could be sending your personal information to identity thieves.

Then, confirm that your security software is active and current: at a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. You can buy stand-alone programs for each element — or a security “suite” that includes these programs — from a variety of sources, including commercial vendors or from your Internet Service Provider. Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software protects against the newest threats only if it is up-to-date. That’s why it is critical to set your security software and operating system (like Windows or Apple’s OS) to update automatically.

Some scam artists distribute malware disguised as anti-spyware software. OnGuardOnline offers a list of security tools from legitimate security vendors selected by GetNetWise, a project of the Internet Education Foundation. Resist buying software in response to unexpected pop-up



MINIMIZING THE EFFECTS OF MALWARE

messages or emails, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers have used to spread malware, and that has attracted the attention of the Federal Trade Commission, the nation's consumer protection agency, as well as a number of state law enforcement agencies.

Once you confirm that your security software is up-to-date, run it to scan your computer for viruses and spyware. Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect.

If you suspect that your computer *still* is infected, you *may* want to run a second anti-spyware or anti-virus program. Some computer security experts recommend installing one program for real-time protection, and another for periodic scans of your machine as a way to stop malware that might have slipped past the first program.

Finally, if the problem persists after you exhaust your own ability to diagnose and treat it, you might want to call for professional help. 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. Your notes will help you give an accurate description to the technician.

If you need professional help, if your machine isn't covered by a warranty, or if your security software isn't doing the job properly, you may need to pay for technical support. Many companies — including some affiliated with retail stores — offer tech support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services — especially if there's a toll-free helpline — but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a technician or 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 to avoid it in the future. If your security software or operating system was out-of-date, download the newest version and set it to update automatically. Use the opportunity to back up important files by copying them onto a removable disc. Other ways to minimize the chances of a malware download in the future:

- **Don't click on a link in an email or open an attachment unless you know who sent it and what it is.** Links in email can send you to sites that automatically download malware to your machine. Opening attachments — even those that appear to come from a friend or co-worker — also can install malware on your computer.



MINIMIZING THE EFFECTS OF MALWARE

- **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.
- **Talk about safe computing.** Tell your kids that some online activity can put a computer at risk: clicking on pop-ups, downloading “free” games or programs, or posting personal information.

Finally, monitor your computer for unusual behavior. If you suspect your machine has been exposed to malware, take action immediately. Report problems with malware to your ISP so it can try to prevent similar problems and alert other subscribers, as well as to the FTC (www.ftc.gov).

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

January 2008