

TELLTALE SIGNS OF A COMPUTER VIRUS INFECTION

by [Dennis O'Reilly](#)

PCs do the darnedest things. When a program crashes, your system slows down, or a file or program refuses to open, it's probably due to a problem with an application or device. But not always. Computer viruses and worms will cause your PC to exhibit many of the same symptoms as a failed or failing component or program.

Here are some of the primary indicators that your system is infected:

- Your system slows to a crawl for no apparent reason.
- The machine crashes, with or without an automatic restart.
- Error messages pop up repeatedly.
- Programs or files open slowly or not at all (especially security apps).
- You can't access drives or other storage media.
- Certain Web sites won't open in your browser, especially those of security software vendors.
- You can't download updates for your antivirus software.
- You can't print.
- A program disappears from your system.
- Strange icons are added to your desktop, or programs appear that you never installed.
- The unused space on your hard drive disappears (which could mean a worm is making copies of itself).

- People in your contacts list receive e-mail from your account, often with a virus attached.
- There's a big jump in the amount of traffic on your network, especially outbound.

How to disinfect a PC

Whenever your system starts acting funky, the simplest remedy is to use Windows' System Restore feature to turn back the clock to a time when the machine worked. (Note that many viruses and worms can outsmart System Restore, so this is far from a cure-all.)

Microsoft's Help and Support site offers step-by-step instructions for using System Restore in XP (which also describes how to undo a restoration). Vista users will find information on System Restore and other system-recovery options for that operating system on the company's Windows Help and How-to site.

Even if System Restore appears to fix your PC, update your antivirus software's definitions and do a full system scan with the program. If you don't use AV software, download and install a copy. You'll find a list of free and low-cost antivirus programs on this [Download.com](#) page. Two freebies that get rave reviews from most users are [Avira AntiVir Personal](#) and [Avast Home Edition](#).

Another option for virus and worm removal is Microsoft's own [Malicious Software Removal Tool](#), which can disinfect a PC but doesn't prevent infections. Note that if your system is set to receive automatic Windows updates, it probably already has the tool installed. You can read more about MSRT on the [Microsoft Help and Support site](#).

Of course, if the virus or worm has blocked your PC's access to the Internet or is preventing your security software from running, you'll have to use another system to download and install an up-to-date antivirus program on a flash drive, optical disc, or other external storage device. Then plug or insert that device in the infected machine and run the AV program from there. One option is the free [ClamWin Portable](#), though many other free AV programs can be installed and run off external media.

Where did the virus/worm come from?

When you're in the midst of a PC disinfection, the source of the virus may not be your first concern. But once your system is working again, you want to avoid whatever action caused the problem.

In the past, most viruses and worms traveled via e-mail and latched themselves onto your hard drive when you clicked to open an attachment, or sometimes when you merely viewed a message. Now infections are more likely to occur after you browse to an infected Web site or download and open a file.

The recent Conficker worm takes advantage of Windows' Autorun feature that allows programs to open simply by plugging in the USB flash drive, CD, or DVD on which it's stored, sometimes even if you thought you had disabled Autorun and AutoPlay on the machine. Microsoft released a patch that closed this hole late last year, though you still must disable these features manually.

Your best virus/worm-prevention strategy is to keep Windows and your antivirus/antispymware/firewall software up-to-date, don't open e-mail attachments you weren't expecting (even if they appear to be from someone you know), and avoid file-sharing and other dicey Web sites. This is no guarantee of keeping your PC virus-free, but it will keep the odds in your favor.