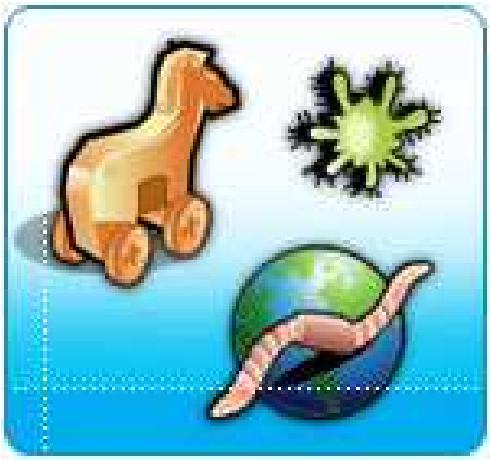
What are viruses, worms, and Trojans?



Viruses, worms, and Trojans are malicious programs that can cause damage to your computer and information on your computer. They can also slow down the Internet, and they might even use your computer to spread themselves to your friends, family, co-workers, and the rest of the Web. The good news is that with an ounce of prevention and some good common sense, you are less likely to fall victim to these threats. Think of it as locking your front door to protect your entire family.

Read on to learn about the characteristics and differences of viruses, worms, and Trojans.

What is a virus?

A virus is a piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. Viruses can damage your software, your hardware, and your files.

Virus (n.) Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or information.

Just as human viruses range in severity from Ebola to the 24-hour flu, computer viruses range from the mildly annoying to the downright destructive. The good news is that a true virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.

What is a worm?

A worm, like a virus, is designed to copy itself from one computer to another, but it does so automatically by taking control of features on the computer that can transport files or information. Once you have a worm in your system it can travel alone. A great danger of worms is their ability to replicate in great volume. For example, a worm could send out copies of itself to everyone listed in your e-mail address book, and their computers would then do the same, causing a domino effect of heavy network traffic that would slow down business networks and the Internet as a whole. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long for you (and everyone else) to view Web pages on the Internet.

Worm (n.) A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding.

Because worms don't need to travel via a "host" program or file, they can also tunnel into your system and allow somebody else to take control of your computer remotely. Recent examples of worms included the Sasser worm and the Blaster worm.

What is a Trojan?

Just as the mythological Trojan horse appeared to be a gift, but turned out to contain Greek soldiers who overtook the city of Troy, today's Trojans are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage. A recent Trojan came in the form of an e-mail message that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.

Trojan (n.) A computer program that appears to be useful but that actually does damage.

Trojans spread when people are lured into opening a program because they think it comes from a legitimate source. To better protect users, Microsoft often sends out security bulletins by e-mail, but these bulletins will never contain attachments. We also publish all our security alerts on our Security Web site before we send notice of them to our customers.

Trojans can also be included in software that you download for free. Never download software from a source that you don't trust. Always download Microsoft updates and patches from Microsoft Windows Update or Microsoft Office Update.

How do worms and other viruses spread?

Virtually all viruses and many worms cannot spread unless you open or run an infected program.

Many of the most dangerous viruses were primarily spread through e-mail attachments—the files that are sent along with an e-mail message. You can usually tell if your e-mail includes an attachment because you'll see a paperclip icon that represents the attachment and includes its name. Photos, letters written in Microsoft Word, and even Excel spreadsheets are just some of the file types you might receive through e-mail each day. The virus is launched when you open the file attachment (usually by double-clicking the attachment icon).

Tip: Never open anything that is attached to an e-mail message unless you were expecting the attachment **and** you know the exact contents of that file.

If you receive an e-mail message with an attachment from someone you don't know, you should delete it immediately. Unfortunately, you're no longer safe opening attachments from people you do know. Viruses and worms have the ability to steal the information out of e-mail programs and send themselves to everyone listed in your address book. So, if you get e-mail from someone with a message you don't understand or a file you weren't expecting, always contact the person and confirm the contents of the attachment before you open it.

Other viruses can spread through programs you download from the Internet or from virus-ridden computer disks that you borrow from friends or even buy in a store. These are less common ways to contract a computer virus. Most people get viruses from opening and running unknown e-mail attachments.

How can I tell if I have a worm or other virus?

When you open and run an infected program, you might not know you've contracted a virus. Your computer may slow down, stop responding, or crash and restart every few minutes. Sometimes a virus will attack the files you need to start up a computer. In this case, you might press the power button and find yourself staring at a blank screen.

All of these symptoms are common signs that your computer has a virus—although they could also be caused by hardware or software problems that have nothing to do with having a virus.

Beware of messages warning you that you sent e-mail that contained a virus. This may mean that the virus has listed your e-mail address as the sender of tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses.

Unless you have up-to-date antivirus software installed on your computer, there is no sure way to know if you have a virus or not. If you don't have current antivirus software or if you're interested in installing a different brand of antivirus software, visit our Security software downloads page.

Next steps: Reducing your virus risk

Nothing will guarantee the security of your computer 100 percent. However, you can continue to improve your computer's security by keeping your software up to date and maintaining a current antivirus software subscription.

What You Should Know About Blaster

The Blaster worm (W32.Blaster.A and its variants) targets a security issue related to the Remote Procedure Call (RPC) function that Microsoft addressed with a released security update. Blaster targets computers with out-of-date software, and those computers remain at risk of infection until the update is installed. We recommend that

customers install the update from Security Bulletin MS03-039 to help protect against this malicious software.

Actions to Take Now

1. Symptoms of Infection

If your computer is infected, your computer may operate normally, may appear sluggish, or may restart every few minutes without your input.

Shutdown error. If your computer is infected, you may see this error message.

If your system is shutting down, follow these steps to stop the cycle. Then proceed to Step 2 to remove the worm.

To end the Blaster worm process

1. Press **CTRL+ALT+DELETE**.
2. Click the **Task Manager** button.

3. Click the **Processes** tab.

4. Click the **Image Name** column heading to sort the processes alphabetically by name.

5. Look for a process named **Msblast.exe**. If you find it, click the name to select the process, and then click the **End Process** button.

6. Close the **Task Manager**.

2. Check For and Remove Blaster

Use the Microsoft Windows Malicious Software Removal Tool to search your hard disk for and remove Blaster variants.

3. Protect Your PC

To help secure your computer against Blaster and other threats on the Internet, follow our Protect Your PC guidance to set up a firewall, get software updates, and use up-to-date antivirus software.

What You Should Know About Sasser

The Sasser worm (W32.Sasser.A and its variants) targets a security issue with the Local Security Authority Subsystem Service (LSASS) that Microsoft addressed with a released security update. Sasser targets computers with out-of-date software, and those computers remain at risk of infection until the update is installed. We recommend that customers install the update from Microsoft Security Bulletin MS04-011 to help protect against this malicious software.

Actions to Take Now

1. Enable a Firewall

Before you take other steps, make sure you have a firewall activated to help protect your computer against infection. If you have a hardware firewall in place for your home or workplace connection, or if you use the firewall included with Windows XP, the Sasser worm is most likely blocked. If your computer has been infected, a firewall will help limit the effects of the worm on your computer. For comprehensive guidance to installing and enabling a firewall, see our Protect Your PC guidance.

2. Install the Required Update

To help protect your computer against Sasser, you must first download and install security update 835732, which was released with Microsoft Security Bulletin MS04-011. You can find update 835732 on the Windows Update Web site listed in the Critical Updates and Service Packs section. You can also download and install this update manually from the Microsoft.com Download Center. To find the download for your operating system, refer to Technical Security Bulletin MS04-011.

Note If you installed the updates for MS04-011 manually or through Automatic Updates before April 30, 2004, then you are already protected against this issue.

3. Check For and Remove Sasser

Use the Microsoft Windows Malicious Software Removal Tool to search your hard disk for and remove Sasser variants.