All about viruses

(modification of original article by Internet ScamBusters)

Stop Viruses In Their Tracks

Perhaps the best thing you can do for your computer—and your peace of mind—is to resolve to protect yourself from computer viruses. Viruses can cost you money and destroy your privacy.

Even if you own a virus-scanning program, we believe you'll learn something new. Let's get started...

Note: This information isn't meant to scare you. It's meant to educate you, so that you can defend yourself properly.

What Is a Computer Virus?

Like viruses that infect living beings, computer viruses infect your computer. They are software, and are often attached to other software or documents you might receive. When you run the virus's software or the file the virus has infected, the virus can infect your computer's software.

There are many types of viruses and terms for them, but we'll use the general term *virus* to make things easy.

How viruses spread

Like the flu virus, a computer virus must spread from host to host to survive. When we get the flu, we cough and sneeze, and tiny particles carrying the virus spread the flu to other people.

With computer viruses, the virus is designed to spread from your computer to other computers. Here are some of the most common ways they spread:

- Once the virus has infected your system, it may automatically send out emails containing more copies of the virus using the address book in your email program. This type of virus is called an Internet Worm, because it is a self-propagating virus. For example, an Internet worm crippled tens of thousands of computers and slowed down parts of the Internet on the weekend of January 29, 2003.
- If the virus is a macro virus (attached to a Microsoft Word document, for example), it may attach itself to any document you create or modify. If you send another document to someone by email, the virus goes along with it.
- Sometimes viruses masquerade as a fun program (like an electronic greeting card) that secretly infects your system. If you pass the program along, not realizing that it contains a virus, you will be transmitting the virus manually to your friends, family, or colleagues.

Trojan Horses

Trojan Horses are closely related to computer viruses, but they differ in that they do not attempt to replicate themselves. More specifically, a Trojan Horse performs some undesired—yet intended—action while, or in addition to, pretending to do something else. A common example is a fake login program, which collects account information and passwords by asking for this info just like a normal login program does.

Malicious and benign viruses

Many computer viruses are malicious; in other words, they can erase your files or lock up whole computer systems. Other computer viruses are more benign; they don't do any direct damage other than by spreading themselves locally or throughout the Internet.

Regardless, computer viruses should always be treated.

More general information about computer viruses

- TJU Computer Virus Information Page: http://www.tju.edu/tju/dis/virus/
- University of Nebraska-Lincoln - Understanding Computer Viruses Pages: http://www.unl.edu/security/viruses/

What Kind of Damage Can Computer Viruses Do?

The damage a computer virus can inflict on your system depends on many things, including how sophisticated the virus is. Here is a short listing of the types of damage viruses can do to your computer; they can really hit you where it hurts:

- Some viruses can delete or change files. Some viruses will delete all of your documents, or even reformat your hard drive, making your computer unusable.
- Some viruses can release confidential information like credit card information, account numbers, and passwords by emailing it to random email addresses or the address of the virus writer.
- Some viruses can slow down your system dramatically.
- Some viruses plant monitoring software or change security settings that allow hackers to enter your computer without you knowing about it and steal information or control it.
- Other viruses, like the Internet worm that hit recently, also can have widespread effects on computer networks and the Internet.

Your Computer May Have a Computer Virus If...

How do you know if you have a computer virus? If you're not running an antivirus program (see the next section), you may not know at all since many viruses are benign.

Some symptoms of a virus infection are:

- Your computer displays strange messages, plays music, or shows odd graphic displays.
- Your computer takes longer to boot up, operates more slowly than usual, and takes longer to start programs.
- Your computer has much less memory or hard drive space available.

Some legitimate software can cause these symptoms, so *the only way you can be sure your computer is virus-free is to regularly scan it for viruses using antivirus software*.

How Can You Protect Your Computer From Viruses?

You need antivirus software to be safe. You should consider the cost of the software as part of the purchase of your computer. It's that important.

After you've installed the antivirus software, you will need to download regular updates that tell the antivirus software about new viruses and how to detect them. Most antivirus software comes with a year's worth of updates, and you can usually set the software to either automatically download the updates, or display a reminder for you to do so.

This is vital since there are over 500 new viruses discovered each month!

Antivirus programs

- Norton AntiVirus and McAfee VirusScan are the two best-known antivirus programs for the Microsoft Windows operating systems.
- If you are strapped for cash, AVG Anti-Virus provides a free version of its antivirus program and free updates for Windows-based computers.
- For Macintosh users, Norton AntiVirus and McAfee's Virex for Macintosh provide protection.
- For Linux users, try RAV AntiVirus.

While the vast majority of viruses are written to infect Windows-based systems, Macintosh and Linux users should still also have virus protection.

Antivirus program features

All antivirus software lets you scan the computer's memory and hard drive for viruses. Depending on the software package, the antivirus program may also be able to protect against:

- Incoming emails and email attachments with viruses.
- Viruses received through instant messaging, such as ICQ.
- Infected downloaded files, before you open the file.
- Attacks against your computer from outside (firewall software).

If you just want to scan your computer for viruses for free *right now*, check out Trend Micro's free online virus scan and McAfee FreeScan.

More information about antivirus software

- Norton AntiVirus: http://www.symantec.com/nav/
- McAfee VirusScan: http://www.mcafee.com/myapps/antivirus.asp
- Virex for Macintosh: http://www.mcafeeb2b.com/products/virex/default.asp
- RAV Anti-Virus (Linux): http://www.ravantivirus.com/
- AVG Anti-Virus (free version available!): http://www.grisoft.com/
- Trend Micro's free online virus scan (requires Internet Explorer version 4.0 or later or Netscape version 3.01 or later): http://housecall.antivirus.com/housecall/start_corp.asp
- McAfee's FreeScan (requires Microsoft Windows and IE 5.0 or later): http://www.mcafee.com/myapps/mfs/default.asp

How Can Your Computer Catch a Virus?

There are only two ways for your computer to get a virus:

- You load the virus onto your computer through an infected floppy, CD-ROM, or other storage medium.
- The virus arrives by a downloaded file, email attachment, or other method from the Internet or a network.

At this point, an infected file is on your computer's hard drive. But remember, your computer will only become infected if you launch or view the file, or run the infected program.

So an important tip is to always scan new files for viruses before you use them.

Precautions to take when working with files and the Internet

- Before you load a file or install software onto your computer from a floppy disk or CD-ROM, use your antivirus program to scan the floppy or CD.
- If you receive an email attachment from an unfamiliar email address, or an attachment you were not expecting, either scan it or delete it (preferred).
- If you receive an email attachment from someone you know, and your antivirus program does not automatically scan incoming emails, save the attachment to your hard drive and scan it with the antivirus program. Your friend or colleague's computer may be infected with a virus.
- When you download software from the Internet, be sure to download it from the software company's site or a recognized download site (http://downloads-zdnet.com.com/, http://www.download.com or http://www.tucows.com for example). Download the file to your hard drive and scan it using your antivirus program before you run or decompress it.
- If someone sends you a joke file or electronic greeting card that you must launch to view, be very wary. Better yet, just don't launch it.
- Make sure your email client software is updated with the most current security patches and service packs applied.

If you use Microsoft Outlook as your email client, and have all the service packs installed, it will block the receipt of known types of attachments that may contain viruses. Additionally, use of the latest version of Norton Antivirus configured to scan your incoming and outgoing email will also catch any known email borne viruses. Outlook should also have its security settings configured to use Restricted sites zone.

More tips and news about threats

More virus prevention tips are available at: http://www.mcafee.com/anti-virus/virus_tips.asp

News about the latest virus threats are available at:

- http://www.symantec.com/avcenter/
- http://www.mcafee.com/anti-virus/default.asp

Your antivirus vendor's website contains information about how to remove a virus. Note that professional intervention may be required due to the fact that a lot of viruses corrupt system files that must be recovered from original install media.

When a Virus Isn't a Virus: Hoaxes and Chain Emails

Every day, forwarded emails from concerned people or friends get sent around the Internet telling the recipient about a new, super-dangerous virus that's unlike anything the Internet has seen before.

Unfortunately, 99% of the time, these forwarded emails are hoaxes.

In fact, most real viruses don't come with email alerts (except from your antivirus software company), whereas almost all these other virus emails are hoaxes.

Much like urban legends, these hoaxes get sent around because they sound so real. But like chain letters, you can stop the hoaxes at the source. Just research the following sites, make sure the email is a hoax, and then delete it.

More information about virus hoaxes

- HOAXBUSTERS Home Page: http://hoaxbusters.ciac.org/
- Symantec Security Response - Hoax Page: http://securityresponse.symantec.com/avcenter/hoax.html
- VMyths.com: http://www.vmyths.com/
- Urban Legends Reference Pages: Computers (Viruses): http://www.snopes.com/computer/virus/virus.htm