Computer Viruses: How to Avoid Infection

Viruses

From viruses to worms to Trojan Horses, the catchall term “virus” describes a threat that's been around almost as long as computers. These rogue programs exist for the simple reason to cause you problems. Once you understand what viruses are and how they can work, you can build a defense.

What’s a Virus?

- A computer virus is similar to the biological viruses that cause disease on a daily basis. Just as a biological virus is a small strand of packaged DNA that’s sole purpose is to invade a host body and use it to replicate itself, so too a computer virus invades a host computer and then replicates itself. Often viruses do damage, slowing down a computer, erasing files, and even damaging computer hardware.

- The term “virus” is a catchall term that actually applies to three different kinds of malicious programs:
  - Viruses
  - Worms
  - Trojan Horses

How Can I Get a Virus?

- Even though there are tens of thousands of viruses floating around the Internet, there are only a few ways that a virus can infect your system. You can catch a virus by doing something, such as installing a program, or by not doing something, such as not keeping your system patched properly.
- Many viruses infect systems if you download and install an infected program. You can obtain the virus-infected file by either downloading it from the Internet, opening an infected e-mail attachment, or using a file-sharing network.
- You don’t always have to open an infected attachment from an e-mail to obtain a virus. Some viruses can infect early versions of Outlook by merely opening an infected e-mail.
- Unscrupulous Web sites will use Java or ActiveX controls to infect machines, often planting viruses on them without warning through a browser and turning them into zombies.
- One key way to get a virus, especially a worm, is by not keeping your system patched against the latest security threats. Hackers discover new vulnerabilities in systems, which vendors, such as Microsoft, constantly patch against. Without the latest updates, your system can be vulnerable to old attacks.

Various Virus Types

- Not all viruses are created equal. What’s commonly referred to as a virus actually can fall into one of three categories. All of them essentially do the same thing. The main difference between the types is the way they infect a system. Knowing

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization
that purchased the TechRepublic CD-ROM on which this form was provided.

the difference between the types of viruses can give you an idea about how they replicate and how to battle them.

Viruses

- Viruses are the names given to small programs that don't usually replicate on their own. You obtain a virus by running an infected program or opening an infected data file. Viruses normally infect program files, which are identifiable by the COM or EXE program extension. Some viruses can also infect batch files such as BAT and CMD files. Occasionally, viruses infect data files. Usually affected data files are Microsoft Office files such as Word DOCs and Excel XLS files. MP3 files have also been mentioned as possible virus sources, although few viruses that exploit MP3 files exist.
- Viruses are spread by passing files from one user to another. You can obtain them via e-mail, by downloading files from the Internet, or by sharing files over the network or via removable storage devices such as floppy disks.
- Some viruses don't carry any payload, meaning they don't cause damage. Most, however, will delete, damage, or alter files. News.com recently reported about a class of viruses that would encrypt important data files and hold the decryption key ransom until the affected company paid the hacker who launched the virus.

Worms

- Worms are more sophisticated programs than simple viruses. Rather than relying on a user to do something, such as open an attachment, to cause an infection, a worm will run and replicate on its own. Very sophisticated worms can also seek out other computers to infect.
- Worms usually exploit security holes inside of computers. Software vendors routinely issue patches to software when such holes are discovered. If you don't keep a system properly updated, you can easily leave your system open to attack. Firewalls also make good defenses against worms because worms will often seek out little-used TCP/IP ports as entry points into a system.
- The Code Red worm is an example of one that exploited a hole in Microsoft's IIS Web server, allowing it to infect Web servers and seek out other unprotected Web servers. Other worms affect Microsoft Outlook and can read your address book and then re-email themselves to everyone on your list.

Trojan Horses

- Like the wooden horse that inspired the name, Trojan Horses trick users into installing them by appearing to be legitimate programs. Once installed on a system, they reveal their true nature and cause damage. Some Trojan Horses will contact a central server and report back information such as passwords, user IDs, and captured keystrokes.
- One common Trojan Horse is called SpyBot. Don't confuse this with the anti-spyware tool of the same name. The Spybot Trojan Horse will infect important configuration and TCP/IP utilities on your system and leave a backdoor for hackers to enter your system from the Internet.

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization that purchased the TechRepublic CD-ROM on which this form was provided.

Computer Viruses: How to Avoid Infection

- **Zombies**
  - The term “Zombie” doesn’t refer to a virus itself. Rather, it’s the term used by hackers to describe computers that have been infected by a class of virus that allows the hacker to control the workstation remotely. Often hackers will use thousands of similarly infected Zombies to launch attacks on other systems—Web servers, Web sites, financial institutions, and so forth. These attacks then form Denial of Service attacks, whereby the target is suddenly overwhelmed by thousands of fast, repeated messages or connections that it can’t handle.
  - Zombie attacks can either bring down a target by causing it to crash under the weight of the attack or can cause it to slow down severely. The target will have such a hard time filtering attacks from legitimate traffic that it will be nearly unusable.

- **Identifying an Outbreak**
  - Your first line of notification about a computer virus is going to be your antivirus software, assuming you have one installed. The exact symptoms of viruses you may have will vary depending on the type of infection. You can keep an eye out for certain things however.
  - Sometimes viruses will trigger windows to appear and disappear randomly on your system as they do their work. These will be very rapid but may include an odd warning or request for you to click OK. If you see bizarre error messages appear on-screen or windows start flashing of their own accord, check with IT.
  - Some viruses can create small data files that fill up hard drive space or allow programs to be downloaded to your workstation, turning your workstation into a network server for pirated files or pornography. If you see a sudden decrease in free drive space, you might have a virus.
  - Viruses can also impact performance of your system by overloading it with additional tasks. This can also be a symptom of spyware, so don’t panic.
  - Viruses can corrupt or damage data files and programs. This can cause you to lose important data or experience error messages and blue screens on your operating system. These can also be indications of hardware failure, although hardware failure is much less likely on newer systems. Check with IT immediately if you experience any of these symptoms.

- **Viruses vs. Spyware**
  - Spyware and viruses can have negative impact on your system. Both viruses and spyware can wreak havoc on your computer. Both invade your system and can cause problems, ranging from slowdowns to errors. Both can report information back to central servers, revealing personal information and surfing activity.
  - Theoretically, spyware comes from legitimate organizations whose main goal is to collect information on your habits. After that, their goal is to display ads from third parties or pass information to people who will send you e-mail about stuff you’re interested in. They’re not trying to cause damage, even though they often do. Viruses do intentional harm with a clearly negative and often illegal goal in mind. Spyware is usually simply annoying.

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization that purchased the TechRepublic CD-ROM on which this form was provided.

Computer Viruses: How to Avoid Infection

Virus Vendors

- Many companies create software to help combat viruses. Some of the most popular of these companies are Symantec, McAfee, Sepbos, Grisoft, Panda Software, and TrendMicro. Our organization uses *Symantec Enterprise Virus detection software*. We chose it because it seemed to have the most extensive coverage for the way in which our network is organized.
- Antivirus clients run on workstations and continually monitor what the computer's doing. When a virus is detected, a warning will appear on the screen, and the software will deal with it. Most software is centrally managed. This means that IT is notified when a virus appears on your screen. Program and virus signature file updates are also handled centrally.

Keeping Virus Scanners Up to Date

- Every antivirus program has a virus signature file. The virus signature file is a database that contains information about viruses and how the antivirus program can detect and resolve the problem. Virus signature files are unique to each antivirus program. You can't share them or read them individually.
- With dozens to hundreds of new viruses appearing on a daily basis, it's important that you keep this file up to date. Your antivirus program can't detect or defend against a virus that's not in its database. Your antivirus program is only as good as its last update. If a virus appears today and you updated last Monday, you can be vulnerable.
- IT tries to centrally manage your virus signature file. The file should be no more than one week old. If it's older than that, you stand a greater chance of having an infection. Certain updates to virus signature files and antivirus program updates may require you to reboot your system. If you get a message saying a reboot is necessary, you should do so as soon as possible.

XP SP2 Security Features

- Windows XP Service Pack 2 added several new security features to Windows XP. First, Microsoft added the Windows Security Center. The Security Center is a Control Panel item that centralizes security information for Windows XP. It checks to make sure that the Windows firewall is enabled and that you've installed and properly updated an antivirus program.
- SP2 updated XP's built-in firewall, turning it on by default. Microsoft added features to the firewall to allow you to selectively enable programs to access the Internet. It can also block worms from entering your system.
- Finally, XP's new update service will check for and download system updates to ensure you've got the latest security and system updates from Microsoft.

Recovering from an Infection

- Recovering from a virus infection can be a nightmare. If your workstation gets infected with a virus, a simple virus scan with your antivirus program should catch and remove the virus.

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization that purchased the TechRepublic CD-ROM on which this form was provided.

- A fast way to recover from a virus attack is to reimage your workstation from a disk image file. This will cause you to lose data and programs installed after the image was created, but it will surely remove the virus. Restoring from a backup may help, but your backup may be infected as well, so you should scan your workstation immediately after resorting from backups.
- After you've run a virus scan and encountered a virus, you should clear XP's System Restore and Precache. The virus may have been backed up into System Restore by XP and it can reinfect your system if you restore from a storage point. Likewise, the precacher helps quickly load programs in XP, so a virus can hide in precache files.
- To clear System Restore, right-click My Computer and select Properties. Click the System Restore tab. Select the Turn Off System Restore check box. Click OK.
- To clear the Precache, open Windows Explorer and navigate to C:\Windows\Prefetch. Click Edit | Select All and then press [Delete].

Virus Hoaxes

- Sometimes you'll get an e-mail from a friend warning you about the "latest virus" to be aware and panicky over. Often times, these viruses aren't real. The effect of the false warnings is threefold: First, they create an unwarranted worry about a potential threat. Second, they may actually make you less likely to believe warnings that crop up about real viruses. Third, they can plug up corporate e-mail servers and clients with wasted messages.
- Even if someone who's into computers warns you about a virus, don't necessarily take it as gospel truth. IT keeps up to date on the latest big virus threats. Check with IT before forwarding warnings to coworkers.
- Most major virus vendors maintain a list of virus hoaxes. You can check with these Web sites to see if a virus is legitimate or a hoax. Some sites include:
  - http://securityresponse.symantec.com/avcenter/hoax.html
  - http://vil.mcafee.com/hoax.asp
  - http://hoaxbusters.ciac.org/

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization that purchased the TechRepublic CD-ROM on which this form was provided.

Computer Viruses: How to Avoid Infection

- **Top Ten Virus Protection Tips When Using Windows XP**
  - Install antivirus software.
  - Make sure updates are current: No more than one week old.
  - Scan your system regularly.
  - Don’t install new programs without first notifying IT.
  - Don’t visit unauthorized Web sites.
  - Don’t open e-mail attachments.
  - Don’t use file-sharing software.
  - Install a firewall on your workstation.
  - Keep your Windows XP system files up to date with all of the current security updates.
  - Check with IT when error messages or warning windows pop up.

Copyright © 2005 CNET Networks, Inc. All rights reserved.
This handout may be photocopied and distributed only within the organization
that purchased the TechRepublic CD-ROM on which this form was provided.