

Surviving VIRUSES & WORMS in Today's Computing Environment

©2001, Radio Gate International, Inc.

You've heard about them...maybe even experienced one of them first hand. They are those destructive computer programs designed to disrupt and set back the economy through the collapsing of corporate computer systems and networks, and corrupt the personal home computers of innocent families. Through this helpful guide by Radio Gate International, Inc., learn some prevention, protection, and eradication techniques in the battle against viruses and worms, and find out how we at Radio Gate can help you in the event of a serious system infection.

What are Viruses and Worms?

It's important for businesses and individuals to understand the different types of threats that are being passed around the Internet in an attempt to infiltrate the system of a vulnerable computer. The most notorious forms of Internet vandalism are computer viruses and worms. The main difference between the two is that viruses are malevolent, while worms are benign (but very annoying).

A computer virus is an unwanted program that, in almost all cases, a user accidentally installs into his or her computer system. It infects part of the system, causing some sort of damage or data loss, and produces copies of itself to spread to other computers. The damage viruses cause can be minor or catastrophic, depending on the intents of their authors. Some viruses have been known to destroy the data structure of an entire hard drive or even to damage a computer's core of its functionality, the BIOS chip. Others simply target and destroy one type of file, such as program executables or documents.

On the other hand, worms do not damage data, but exist only to reproduce themselves and spread to other computers. Worms are mainly an annoyance and normally do not disrupt the day-to-day use of your computer. However, if a worm happens to infect a corporate network, it has the ability to bring down the company's computers by sending off a deluge of interoffice email.

So why do people make viruses and worms?

Well, some do it just for fun, and to see if they have the programming ability to write a destructive software application. Some are genuinely looking to create chaos, while others have far worse intentions. Some authors build viruses to get information from their victims. The virus returns to the author information stored on your system as it moves on its destructive path.

How a Virus Works

Most of the viruses that cause trouble are transmitted through email. Let's take a look at how these programs transmit themselves quickly.

Let's say you receive an email from a friend that contains a message that reads something like this: "Hey, I found this cool application on the net so I passed it along to you! Tell me what you think." Thinking nothing is out of the ordinary, you click the paper clip icon and download the application to your machine. Once the transfer stops, you open up the application you just downloaded and maybe a cute animation starts to play. Once it finishes, you think, "That was nice," and you go about your business. Little do you know that you were just infected with a virus.

So what happens from here? The first thing is that the virus will probably attack your email address book, mailing itself to all your friends without your knowledge. Now all of your friends think you sent them a cute little animation program when there really is much more to it than that. This is how email viruses are transmitted to millions of people in such little time. In the mean time, the virus is already working on your own system, and the next time you boot up your computer, you could be shocked to find that it doesn't work correctly.

PREVENTION

Computer viruses and worms share the same characteristics as biological viral and bacterial infections. Some computer viruses exist only to duplicate themselves while others attack and corrupt files on your system, and can sometimes make your hard drive inaccessible. Yes, your computer can become ill!

What can you do?

- Never open attachments that you aren't expecting. Email the person who sent it to you and ask if it is free of viruses. It is also not a bad idea to run it through your own virus-checking program just to be sure.
- Make sure you have anti-virus software and keep it up-to-date.
- Keep your eyes open for viruses in attachments ending in ".exe," ".vbs," ".scr" and ".zip." You might want to make it a company policy to not download files of these types without permission from a supervisor. Also, watch out for Microsoft Office documents ending in such extensions as ".doc," and ".xls." These files can contain macro viruses, or programs that run within another program.
- It is *generally* safe to say that attachments ending in ".eml," ".txt," or ".mid," are safe, but still be cautious.
- On average, 10-15 viruses are created each day. Even if your anti-virus software is up-to-date, don't rely on it to stop the newest viruses. Anti-virus software needs information about a virus before it can recognize it, and this information must be published and made available for everyone to download. Once downloaded, you have a defense against that particular virus or worm, but until then, don't open suspicious email attachments, and listen to claims that viruses are circulating, whether you think it's a hoax or not.

As if you haven't been scared enough, there are also rare viruses out there that can be activated without opening any attachments. These viruses take advantage of security holes in mail clients, namely Microsoft Outlook™ and Outlook Express™, and in some cases they can find their way into your computer through web pages viewed with Microsoft Internet Explorer™. These security holes have been recently addressed and fixed, and you can get updates on the Microsoft home page: www.microsoft.com.

Remember, 99.99% of the viruses out there must be run by YOU in order to infect your computer. If you get a virus e-mailed to you, you're generally safe reading the body of the e-mail message, **JUST DON'T RUN THE ATTACHMENT!!** A virus can't infect your computer until you give it your consent (well, unless someone hacks into your machine and runs it, but that's another newsletter).

If you do get a file that you suspect contains a virus, just delete it.

Although e-mail viruses are by far the most common, you can still get infected in any number of other ways. In this last section of our virus guide, we'll look at keeping you safe from as many virus sources as possible.

Other Virus Sources

- Unknown download sites - Be careful when downloading software from the net, especially from a virtual shareware library. A virtual shareware library is a site that has software listings on it, but they don't keep the software on their server. Just hover your mouse pointer over the download link and look at the bottom of your browser. If the URL shown is not the same as the site's it's a virtual shareware library. Most shareware sites are. This isn't to say that you're going to get a virus by downloading software from them. In fact, I've never had a problem (and I download tons of software). What I normally do is try to go to the software's web page. If it seems to be a trustworthy company, I download. Then I double-check the file with my anti-virus software.
- Floppy Disks - Passing around floppy disks use to be the number one way of getting a virus, but it isn't as common as it used to be. In general, just be careful about running programs on floppy disks, especially those from questionable sources. Another thing to be careful of is floppy boot sector viruses. If you have an infected floppy with this type of virus on it, you'll be infected if you forget to take it out of your drive when you re-boot your computer. To avoid problems, just don't leave floppy disks in your drive.
- Macro Viruses - I had mentioned this briefly earlier. Be careful with MS office documents that come from questionable sources. They can contain what's called a macro virus. These can delete files, alter program menus, and more.

Unfortunately, these are relatively easy to write, so they are among the most widespread variety of viruses. Be extremely careful when opening unknown MS office files, especially Word documents. Probably a good idea to save these files to disk then check them with your anti-virus software before opening them.

Well, that's about it. I know we could easily fill a book discussing viruses, but I'm just tryign to pass along the basics.

Just remember, keep your anti-virus software up to date and don't run / open any files you don't trust 110%.

PROTECTION

Your first step in protecting your PC from viruses--and also from any other form of system failure--is to make frequent backups of your important data on removable media (such as floppies, CD-Rs, Zip disks, LS120 SuperDisks, or some other form of writable storage). However, if you have more than a few files to back up, copying them to removable media is a chore. While most hardware comes with backup programs designed to help you make copies of your data, there are a number of applications dedicated simply to data protection and recovery.

Some backup applications, like Roxio GoBack 3.0, concentrate on quick system recovery in the event of data corruption, viruses, or other hazards. GoBack takes periodic "snapshots" of critical areas of your hard drive and stores them; should something go awry, you can revert your system to its state when one of the snapshots was created. Note, however, that GoBack doesn't actually create backup copies of your files. While it's a useful recovery tool, your data still isn't safe from a catastrophic hardware failure, or a virus that completely wipes out your hard drive.

Other apps, like Norton Ghost 2002 and PowerQuest Drive Image 4.0, create images of all or parts of a hard drive, which is useful for a variety of tasks beyond simply creating backups. For instance, they make upgrading your hard drive a simple process, and in business environments they can help to quickly initialize a number of identical computers. Restoring full images is incredibly simple, and recovering individual files from images only requires you to use a simple browser-style application to select the files to be restored. The only downside of these programs is that they are geared more toward data manipulation than creating frequent, consistent backups.

The actual task of creating backups is best served by a traditional backup program such as Veritas Backup Exec Desktop Pro 4.5. This program lets you back up files from one system or from a number of PCs across a peer-to-peer network. Its scheduling applet lets you run automated, unattended backups, and its disaster recovery tools let you not only restore files, but also re-create the drive's partition and file-system information (a common target of malicious viruses) should it become corrupted. With reliable backups, your data is safe from viruses and all sorts of other dangers. That doesn't mean viruses aren't a threat, however.

Keep Your PC Healthy

The best way to recover from a virus is never to catch one. Just as you should wash your hands a lot during cold season and try to avoid sharing silverware with sick people, you should also take preventive steps to protect your PC from virus infection.

If you use e-mail, download files from the Internet, or share files with other computers, you should own a good antivirus utility. Among the finest available are Norton AntiVirus 2002, McAfee VirusScan, Panda Antivirus, and others. Better yet, many of these applications are available for download, so you can start protecting your system immediately. Symantec's Norton AntiVirus is widely considered the de facto antivirus suite, although most antivirus programs share a similar set of core features. They can scan your computer's boot areas and file systems for known viruses, check e-mail for malicious attachments as each message arrives, download updates automatically, generate emergency boot diskettes in case of a serious infection, and more.

Most antivirus makers offer different products depending on users' needs. Offerings vary from small, one-user programs for home users and very small businesses to network-monitoring powerhouses for large businesses. For the latter, virus protection should be left to the IT department or network administrator. Software licenses are a great option for businesses that need to protect a network of PCs. However, if you need more than one copy of a product, but aren't ready to purchase a license, Symantec 5- and 10-user multipacks are great options for small companies. In addition, if you're running a small network, you may want to look into a program Veritas Backup Exec Desktop Pro 4.5. As mentioned earlier, programs like Backup Exec can be used to protect personal computers; however, they are also quite effective when used to back up small networks and protect data from the hazards of hard disk failure, power surges, and human error.

Trojans and DOS Attacks

Though they're often lumped together with viruses and worms, trojans are very different. Trojans are small, innocent-looking programs that, once executed, allow intruders to assume partial or full control of an Internet-connected computer remotely, from their own PCs.

Trojans are often used in conjunction with denial-of-service (DOS) or distributed denial-of-service (DDOS) attacks, which are discussed below. In most cases, you can easily avoid a trojan infestation in the same way that you can thwart viruses or worms: by not opening suspicious e-mail attachments from both unknown and familiar parties. Trojans are often found in downloadable software from questionable sources, such as hacker sites and warez (illegally reproduced commercial software) servers.

More sophisticated than worms, viruses, and trojans are denial-of-service (DOS) attacks. These aren't programs at all, but actions undertaken by nefarious parties that result in the inability of users to perform common Internet-related functions, like downloading their e-mail or accessing a Web site. The most common form of DOS attack involves hackers triggering dozens, hundreds, or even thousands of bits of false data packets toward a particular Web site. The attack is intended to cause so much false traffic that legitimate users are unable to access the site.

Unbeknownst to you, your computer may even assist such attacks. A particularly nasty form of DOS assault, called a distributed denial-of-service (DDOS) attack, involves hackers controlling

unsuspecting PCs all over the Net through the use of trojans. A hacker or group of hackers will trigger trojan-controlled computers to simultaneously send massive amounts of false data to the same target. The result is usually tons of data overloading a Web address, choking off real traffic and sometimes crashing the targeted Web server. The best way to prevent this from happening is by installing a firewall, or a program designed to block unauthorized access to and from your computer or network. See more on firewalls in the last section of this guide.

Defend Yourself

You don't have to be a victim of a virus attack, a pawn in a worm's reproductive cycle, or an unknowing assistant in a DDOS attack. By using common sense and installing protective software such as antivirus programs and firewalls, you can prevent your PC from falling victim to hackers' dubious activity. In addition, if you are responsible for protecting your company's network of PCs, you may want to check out our [Licensing Center](#) for more information on volume licensing of software programs.

Your first line of defense against unseemly Internet activity should be to adjust your own habits:

Don't open e-mail attachments from people you don't know—even viruses like the famous Love Bug aren't dangerous until a user activates them, usually by opening an e-mail attachment.

If you receive an e-mail with an attachment from someone you do know, check the file's extension before proceeding. Image files (with extensions like .JPG, .GIF, .BMP, and such) are usually safe to open, as are text files (which have the extension .TXT). Files that may be dangerous are program executables (.EXE, .BAT, .COM, .PIF), Microsoft Word documents (.DOC), and Visual Basic scripts (.VBS). Never open a .VBS file. Delete the e-mail immediately.

Regardless of the attachment's extension, save it to a folder on your hard drive and scan it with an antivirus program before you open it.

When you download files and programs, scan them with your antivirus program before executing them.

What If You Get a Virus?

Don't panic!

If a virus does crawl into your computer, your antivirus software will inform you of your options. Often, an antivirus program can remove viruses from files or boot areas without the need for any further recovery. You may have to boot your system with the emergency diskettes the program made for you.

Sometimes, your antivirus program won't be able to purge an infected file of its virus. The file should be deleted and replaced with a clean copy. Your antivirus software will help you through the process.

Even if you don't already have antivirus software installed when a virus infests your system, such programs can still help you rid your PC of the intruder. If your computer starts acting funky (popping up errors for no apparent reason, reporting file corruption, asking for a third cup of coffee, etc.), grab an antivirus program and give the system a thorough checkup. Programs like Norton AntiVirus 2002 and McAfee VirusScan 5.0 are available for immediate download, so you can start fighting your bug as soon as it rears its ugly head. You may also want to check out the "Back Up Your Data" section in this guide to find applications that will help you restore lost data.

Firewalls

As more and more homes contain multiple computers, it's becoming popular to network them together and share a single broadband Internet connection. Whether you're enjoying such a setup or you have single Internet-connected PC, you should consider investing in a personal firewall.

Firewalls block unauthorized access to and from your computer or network. Information is transferred to and from your PC via open ports, which are basically data conduits. Firewalls block vulnerable ports that can be used by hackers to control your system with trojans or perform other malicious tasks. As such, firewalls are especially useful in preventing your computer from taking part in a DDOS attack, or from being accessed by hackers even if you've already unknowingly installed a trojan.

Among the best and user-friendliest firewalls available are Norton Personal Firewall and McAfee Firewall. If you don't have any Internet security programs yet, check out Norton Internet Security--it's an outstanding buy that includes a firewall, an antivirus program, and more. Norton Internet Security 2002 is also available for download in our Software Downloads Store.

Call Radio Gate!

(Info about how RGI can help needs to go here.)

References

"Virus Guide." *WorldStart.Com Computer Tips, Software, and Web Design*. worldstart.com. Online. 29, Oct. 2001.

Durham, Joel Jr. "Virus Survival Guide." *Amazon.Com*. amazon.com. Online. 29, Oct. 2001.