14 Household Ways To Protect Your Computer From Viruses - by Marv Ko

Computer viruses are deadly. They often spread without any apparent contact and can be a nuisance, or even worse, fatal to your computer. Individuals who create these viruses, estimated at 10-15 new ones a day, are the electronic version of terrorists. Their goal is to inflict havoc and destruction on as many people as possible by disabling, stealing, damaging, or destroying computer and information resources. Often, they have no specific target in mind, so no one is safe. If you access the internet, share files or your computer with others, or load anything from diskettes, CDs, or DVDs onto your computer, you are vulnerable to viruses.

Fortunately, there are good guys working just as hard as the hackers to develop cures for viruses as quickly as they send them off into cyberspace. And there are many things you can do to keep your computer from catching viruses in the first place.

Defining Viruses:

A virus is a small computer program that can copy and spread itself from one computer to another, with or without the help of the user. However, viruses typically do more than just be fruitful and multiply, which is bad enough in itself because it hogs system resources. Anything else viruses are programmed to do, from displaying annoying messages to destroying files, is called their payload. Often, they cannot deliver their payload until an unsuspecting user does something to make the virus execute its programmed function. This could be as simple as clicking on an innocent looking file attachment with the .exe (executable) extension.

Catching a Virus:

Most viruses are spread through e-mail attachments because it's the easiest way to do it. Although Macintosh, Unix, and Linux systems can catch viruses, hackers are particularly keen on exploiting the security weaknesses in anything Microsoft, particularly Microsoft Outlook and Outlook Express. Because of the popularity of this software, hackers get maximum bang for their buck, and they probably get some satisfaction from continually reminding Microsoft that being big doesn't mean you're perfect.

Solution 1: Anti-virus Software

Your first line of defense is to install anti-virus software. To be extra safe, also install firewall software, which is now included in some anti-virus packages. This software can scan all of your drives for viruses and neutralize them. Here are some features to consider when evaluating anti-virus software.

- Compatibility with your operating system - Make sure the software works with your system, particularly if you are using an older operating system like Windows 98.

- Firewall software - If it's not included, find out if it's available. If you must, buy it from another vendor.

- Automatic background protection - This means your software will constantly scan behind the scenes for infections and neutralize them as they appear. This provides some peace of mind.

- Automatic, frequent updates - Because new viruses appear every day, you'll want regular updates. It's even better if they occur automatically when you connect to the internet. If automatic updating isn't included, you'll have to check the vendor's website and download updates yourself. This is vitally important, because you will not be protected from new viruses if your software is out of date.

- Disaster recovery - Software with a recovery utility to help you get your system back to normal after a virus attack is always good to have.

- ICSA certification - The International Computer Security Associatioin has standards for the detection rates of anti-virus software. Make sure your software has the ICSA certification.

- Technical support - It's a good idea to select a package that offers free technical support, either online or through a toll-free number. If you're ever felled by a virus, you may need it. Some anti-virus software vendors are Symantec Corporation (Norton AntiVirus), McAfee Corporation (McAfee VirusScan), Trend Micro Inc. (PC-cillin), and Zone Labs Inc. (Zone Alarm Suite).

Solution 2: The Virus Scan

If you receive a particularly juicy attachment that you're dying to open, save it on your Windows desktop and run your anti-virus software on it first. To do this, click once gently on the file on your desktop ... don't actually open it ... then right click and choose Scan with (Name of Anti-Virus Software) to activate a virus scan.

If it's infected, your anti-virus software may neutralize it, or at least tell you the attachment is too dangerous to open. On the other hand, don't feel guilty if the very thought of saving a potentially damaging file anywhere on your system is enough to quell your eagerness to open it and make you delete it immediately.

Solution 3: Delete first, ask questions later.

When in doubt about the origin of an e-mail, the best thing to do is delete it without previewing or opening it. However, some viruses, such as Klez, propagate by fishing in people's address books and sending themselves from any contact they find to another random contact. You can spread a virus just by having people in your address book, even if you don't actually e-mail them anything. They'll receive it from someone else in your address book, which really makes life confusing. Because of the proliferation of porn on the internet, e-mail viruses often tempt victims by using sexual filenames, such as nudes.exe. Don't fall for it.

Solution 4: Beware of virus hoaxes

E-mails warning you about viruses are almost always hoaxes. You may be tempted to believe them because you typically receive them from well-meaning friends, who received them from friends, etc. These e-mails themselves usually aren't viruses, but some have actually fallen into the hands of hackers who loaded them with viruses and forwarded them merrily on their way as a sick joke.

The proliferation of e-mails about virus hoaxes can become nearly as bad as a real virus. Think about it, if you obey an e-mail that tells you to forward it to everyone in your address book, and they THEY do it, and this goes on long enough, you could bring the internet to its knees. If you ever want to verify a virus warning, your anti-virus vendor may have a list of hoaxes on it website. It's in the business of providing the fixes, so it will know which viruses are real.

Solution 5: Beware of filename extensions

The extension of a filename is the three characters that come after the dot. Windows now defaults to hiding filename extensions, but it isn't a good idea. Just being able to see a suspicious extension and deleting the file before opening it can save you from a virus infection.

To see filename extensions in all your directory listings, on the Windows XP desktop, click Start button | Control Panels | Folder Options | View Tab. Clear the check box for Hide extensions of known file types. Click Apply | OK. System files will still be hidden, but you'll be able to see extensions for all the files you need to be concerned with. Viruses often live on files with these extensions - .vbs, .shs, .pif, .Ink - and they are almost never legitimately used for attachments.

Solution 6: Disable the .shs extension

One dangerous extension you can easily disable is .shs. Windows won't recognize it and will alert you before attempting to open an .shs file. The extension is usually just used for "scrap object" files created in Word and Excell when you highlight text and drag it to the desktop for pasting into other documents. If this isn't something you ever do, or you have Word and Excell 2000 or later, which allow you to have 12 items on the Clipboard, click the Start button | Control Panel | Folder Options | File Types tab. Under Registered file types, scroll down and highlight the SHS extension. Click Delete | Yes | Apply | OK.

Solution 7: Dealing with double extensions

When you turn on your extensions in Windows, you'll be able to detect viruses that piggy-back themselves onto innocent looking files with a double extension, such as happybirthday.doc.exe. NEVER trust a file with a double extension - it goes against Nature.

Solution 8: Beware of unknown .exe files

A virus is a program that must be executed to do its dirty work, so it may have an .exe extension. Unfortunately, this is the same extension used by legitimate program files. So, don't panic if you find files named Word.exe or Excel.exe on your system - they're your Microsoft software. Just don't EVER open any file with an .exe extension if you don't know what the file's purpose is.

Solution 9: Watch out for icons

Viruses in attachment files have been known to assume the shape of familiar looking icons of text or picture files, like the wolf in the hen house. If you recieve an unexpected attachment, don't open it without first running it through your anti-virus software.

Solution 10: Don't download from public newgroups

What better place for a hacker to lurk and stick his virus than in the middle of a crowd? Sooner or later, someone's bound to download it and get the virus going. Don't download files and programs from newsgroups or bulletin boards, or open attachments sent from strangers in chatrooms ("Let's exchange pictures!") without first scanning with your anti-virus software.

Solution 11: Avoid bootleg software

This may seem like a no brainer, but sometimes that tiny price tag on a popular but expensive package can be too good to resist. Resist it! Likewise, be careful about accepting application software from others. You don't know where it's been, and what may have started out as a perfectly clean package could have become infected during installation on someone else's infected computer.

Solution 12: Protect macros in MS Word, Excel, and Powerpoint

A common type of virus uses macros. Macros are sets of stored commands that users can save as shortcuts to perform long functions in just a few keystrokes. A macro virus may perform such mischief as changing file types from text files or spreadsheets into templates, locking up keyboards, and deleting files. Word, Excel, and PowerPoint come with macro virus protection. To make sure yours is activated, open each application, then click Tools menu | Macro | Security. On the Security Level tab, make sure Medium or High is selected. Clcik OK. If you are already infected with a macro virus, you may find that the steps of this procedure are unavailable becasue the virus has disabled them. In that event, run a virus scan on your system to see if your anti-virus software can kill the virus.

Solution 13: Use passwords

If you share your computer, it's a good idea to assign everyone a password. Passwords should be a combination of letters and numbers no less than eight characters long, and preferably nonsensical. Never write passwords and stick them anywhere near the computer. To assign passwords in Windows XP, click the Start button | Control Panel | User Accounts. Follow the prompts to assign/change passwords.

Solution 14: Update application software

Microsoft constantly issues patches for the security holes in its operating system and applications software. however, don't be lulled into complacency if you have Windows Update automatically checking things for you. Update checks for patches to repair bugs in the operating system, not for security problems.

To get the latest security hotfixes (as Microsoft calls them), visit www.microsoft.com and look for hotfixes for all your Microsoft software, particularly Outlook and Outlook Express.

Microsoft also has a free downloadable package called Microsoft Baseline Security Analyzer (MBSA) that scans your system for missing hotfixes. It works with Windows 2000 and XP Home and Professional only. It doesn't support Windows 95, 98, or ME.

To download the MBSA, go to the TechNet section of the Microsoft Website. Be warned that the information is written in techie language, so you may find it daunting.

Last Words:

Now that you know some ways for avoiding and dealing with viruses, let's wrap things up with some solution you've probably heard before but have ignored.

- Back up your files regularly - If a virus crashes your sytem, you'll feel much better if you've got backup copies of all your important files. Make the backup copies on a media that's separate from the computer, such as on diskettes, CDs, or zip disks. Scan them for viruses before you put them away to make sure they aren't infected. If they are, they'll do you no good if you ever have to use them because they will just transmit the virus right back onto your computer.

- Make a boot disk - Create an emergency boot diskette before you have a problem so you can start your computer after a serious security problem To make a boot diskette with Windows XP, put a blank floppy disk in the drive. Open My Computer, then right click the floppy drive. Click Format. Under Format options, click Create an MS-DOS startup disk. Click Start. Keep the disk in a safe place. With luck, you'll never need to use it.

- Turn off you computer - DSL and cable connections that are "always on" may be convenient, but you should always turn off your computer when its not in use. Hackers can't get to a machine that's powered off.

Marv Ko has many years of experience in business, marketing, security, writing, and varied hobbies. He is is the senior editor of www.upublish.info ... your source for Original Content Articles.

Article Source: http://www.articlecube.com