Staying Vigilant in Virus Country

How many times have you received a virus in your e-mail inbox? Probably many times! How many times has a virus contaminated your machine? Hopefully none. Let's keep it that way. Here are some tips to avoid viruses and keep your computer running in top shape.

Viruses are e-mailed as attachments, they are not embedded within the text of an e-mail. If you do not open the attachment, your computer will not be infected. Stay vigilant by doing the following:

■ **Upgrade and update your antivirus software regularly.**
You should buy a new version once a year, and update it once a week. Antivirus company Symantec estimates that 10-15 new viruses are discovered every day. Keeping your software current is crucial; the weekly updates guard against the daily onslaught of new viruses, and buying new software every year will protect your computer from viruses that the older software (even if updated religiously) cannot detect. Most viruses are targeted towards PCs, but Macs should also be updated because there are viruses that target them, and the possibility of cross-platform viruses (that infect both PCs and Macs) is quite real.

■ **Do not open attachments from people you don't know.**
Attachments can be disguised. You might think someone sent you an image, but it could be a virus cleverly disguised as *nyc.gif.pif* or *jane.scr.jpg*. Some e-mail programs will hide the the last extension, revealing only *nyc.gif*. Viruses can also be embedded in Microsoft Word documents and spreadsheets, but are often 'executables' or programs containing extensions like *.pif*, *.exe*, *.vbs*, and *.scr*.

■ **Be wary of e-mail attachments even from people you know.**
Scan attachments with an updated virus program. What if the virus sent itself using the person's address book? Or what if they didn't know they had a virus? There may also be cues in the way it is written, especially if uncharacteristic for the sender. Just last week I received an e-mail from a coworker saying only, "Please open the attach." (Very different than her usual e-mails!) It's important to know that it is not enough to have anti-virus software on your PC, you will also have to run it. You may also want to setup a free e-mail account that you can use for subscriptions or other unnecessary e-mail. I have a free Yahoo account and frequently take advantage of their e-mail scanning utilities.

Senders can disguise their identity in an e-mail. Beware of messages from Microsoft that claim to contain the latest patch (Microsoft never e-mails attachments), or messages that look like they are from your IT department but are written vaguely and have an attachment. One of the latest viruses I received claimed to be from the Wavian IT department, warning of issues with my account. Since I am my IT department, I knew this was fake. The sender managed to create a program which will customize each e-mail to capture your domain and make it look authentic – for example, from 'admin@earthlink.net' or 'staff@mindspring.com' or 'help@aol.com.' Pretty sneaky, eh?

■ **Be very careful of what you download from the Internet.**
Only download programs from reputable sites that you trust. Note that downloading screensavers and other neat programs can sometimes interfere with other programs on your machine, making it unstable… and this could have nothing to do with a virus. Be careful with what you choose to download.

■ **Beware of hoaxes.**
Some e-mail hoaxes will instruct you to check your machine for a certain file; supposedly if you have it, you have a virus. Beware of doing this – you could delete a necessary system file. Confirm hoaxes at www.vmyths.com.

■ **Guard your personal information.**
This is not directly related to viruses, but can be an e-mail created with malicious intent! Never click a link leading you to a website where you have to update your information and provide a credit card. Scammers can fabricate a website to look identical to a company, and can even disguise the link to make it look authentic. I received an e-mail saying that Ebay wanted to update my personal information but it was bogus. The best way to tell is to open a completely new browser (Netscape, Internet Explorer, etc.) and type the URL in by hand. (A URL is the site address [Uniform Resource Locator], like www.wavian.com, or www.amazon.com.)

More tips for staying safe against viruses can be found at www.claymania.com/safe-hex.html (*with* hyphen).

<u>Computer Maintenance</u>

There are also procedures you should follow to keep your computer running in top shape so it is less vulnerable to viruses and data loss. Do these steps once a week, in this order *(instructions for how to do each step are at http://netsquirrel.com/fabfive.)*:

■ **Update your operating system (OS).**
Updating your OS closes the security holes in it. Every OS has known vulnerabilities, and when manufacturers discover these, they make patches that close them. If you have a Windows machine, you only need the 'critical' updates. Visit http://windowsupdate.microsoft.com. When you run the update, it will automatically scan your computer for the updates and patches that you need. To update your Apple computer, visit www.apple.com/support/downloads.
.

■ **Run ScanDisk/DiskFirstAid.**
ScanDisk comes with Windows, DiskFirstAid comes with Apple systems. Both scan the hard drive to update the clusters where your files and programs are kept. If you don't run this utility, your computer may become more like you and forget where the keys are! Help your computer remember where everything is by running this weekly.

■ **Defragment your hard drive.**
Defragmenting your hard drive helps move file clusters closer together. As you delete files and create new ones, gaps are created. If you close these gaps, it cuts down on hard drive wear and tear. Also, according to PC World, May 2002 (pg. 77), "The more fragmented the files on your hard drive are, the more likely a disk error is to destroy them." Defragging takes a long time, however. Run it when you leave the office or before going to bed.

■ **Backup Data.**
Always make sure your data is backed up. If your hard drive failed (and this happened to me twice in the past 4 months), it would be a disaster to lose all of your work. (Luckily, I have OCD when it comes to backing up; it was more of a pain than a disaster.) Keep a list of programs that you use and make sure you everything you need to rebuild your workstation. If your hard drive does fail, there are companies that can try to recover your data. It's not guaranteed that they will succeed, however, and is often expensive. I have a list of companies that will try to recover your data at http://www.wavian.com/web-resources.html#techsupport.

What if you have virus?

There is a lot of information on what to do if you have a virus. In some case, disinfecting your computer using your virus software can make it unstable, and in some other cases, formatting your hard drive can be unnecessary, and also may remove everything *except* the virus. Terrific information on how to deal with a possible virus is at www.claymania.com/panic.html. Print out a copy of their recommendations so you have It handy if you need it.

Holly Russo has been designing web pages and avoiding viruses since 1994. She can be reached at Wavian Web Design, www.wavian.com. Want to receive tidbits and useful information by e-mail? Send a note to russo@wavian.com and ask to be added to Wavianwire.