

Kicker: Practicing Safe Hex

Head: Computer Virus Facts and Fictions

Deck: A real virus can play havoc with your PC, but even a hoax can be a major hassle.

BY CARROLL S. LEVISON

The recent deluge of virus warnings has struck fear in the hearts of techies and novices alike, and rightly so. A virus infection can disable your computer, wipe out your hard disk, and require hours of effort to eliminate. Just as deadly, you may be an inadvertent carrier and spread the virus to your colleagues and clients.

The good news is that many of the recent viruses scares have been hoaxes. The bad news is that you may spend manpower and bandwidth protecting yourself and letting others know about the "danger." The goal of a hoax virus is to get everyone excited about it and then waste lots of resources talking about it.

Understanding how viruses do and do not work will go a long way to easing your fears and helping you take appropriate action. Almost all true viruses require an action on your part before you get infected. You must launch something (open an attached document or execute an attached program) before the virus can harm you. With very few exceptions, just reading an e-mail will not transmit a virus to your computer. Only if you have modified your mail program to read mail using Microsoft Word and have disabled macro virus protection and enabled auto execution of all attachments are you vulnerable. Most people who swear they got a virus from reading an e-mail did so because they opened up an attached file.

Sometimes, it's easy to be deceived. A virus-infected attachment is labeled as a cute screen saver, a funny joke program, a cute picture, an important document or spreadsheet, or even pornography. Thinking the file is legitimate, people open it and find that they are subsequently infected with a virus. In fact, this strategy is so common that viruses are often called "Trojans," after the Greek "gift" that brought the downfall of Troy.

How do you protect yourself from real viruses? By following these "Easy Guidelines to Safe Hex," you get all the fun and productivity of Internet interaction, without the risks. (For the uninitiated, "safe hex" is a geek play on words, combining "safe sex" advertising and "hexadecimal," a numbering system used for coding programs and computer storage.)

1. get educated
2. educate your partners
3. use protection
4. don't take unnecessary risks
5. treat infections promptly

Safe hex 1: Get educated. You don't have to be a computer genius to be knowledgeable about computer viruses. The Internet is crammed with information about how to recognize viruses, how to protect yourself, and how to cure yourself. The following sites contain everything you would ever want to know about viruses and are not too difficult to read or understand.

Carnegie-Mellon CERT Coordination Center Computer Virus Resources
http://www.cert.org/other_sources/viruses.html.

NBCI Anti-Virus Education Page
<http://members.nbc.com/kbechtel/edu.htm>

Sophos Virus Info Page
<http://www.sophos.com/virusinfo/whitepapers/prevention.html>

Symantec Virus Encyclopedia
<http://www.symantec.com/avcenter/vinfodb.html>

Safe hex 2: Educate your partners. You may find that you receive virus alerts from your friends. These alerts are very well intentioned and show they really do care about you. However, your friends may not realize that many of these alerts are hoaxes. Before you start countermeasures, check the "Symantec Virus Encyclopedia" or other source to see if the culprit is a real virus or not. If you get frequent false alarms from one or two sources, you might also want to send your friends the link to the encyclopedia and to this article.

Safe hex 3: Use protection. Proper protection is the key to staying virus free. I personally run active virus-protection software on all of my computers. Widely used programs include Symantec's Norton Anti-Virus (www.Symantec.com), Trend Micro's PC-Cillin products (www.antivirus.com), and McAfee's Virus Scan (www.mcafee.com). Which program is best? It's hard to pick one winner. You will find many articles at the sites listed above to help you evaluate the different anti-virus programs.

If you are cheap like me and don't want to buy your own virus protection, you can download some free programs from the Internet. You will get a long list of web-based and downloadable virus checkers by searching sites such as Yahoo! For a quick web-based virus scan of your hard drives, use Trend Micro, Inc.'s free Housecall program.
<http://housecall.antivirus.com/>

It's also critical to keep your virus protection up to date; old virus programs are ineffective against the latest viruses. Most anti-virus software programs make regular updates of the signature file (which identifies the virus) available for download at the manufacturer's Web site. Some programs can be set to do updates automatically; some can be set to give you reminders; and some you just have to do yourself. Whichever way you choose, just make sure you do it.

Safe hex 4: Don't take unnecessary risks. First and foremost, know who your communication partners are and what their level of knowledge is. A person who is not very knowledgeable about "safe hex" practices is more likely to have a virus infection and to send you a file with a virus in it.

Reduce your risk by making sure you know where a file you receive came from and what it is supposed to be before you open it. Here are some basic guidelines about file types and their level of risk.

Type	File Extension	Risk Analysis
Executable	.exe	Executable files always have the highest risk of containing a virus. You should be absolutely sure of what is in the program and what it does before you open it. I highly recommend scanning an executable program for a virus even when it comes from a reliable source.
Screen Saver	.scr	Screen savers often contain viruses. It is very easy to insert code in these files that can do damage to your computer. Always scan screen savers for viruses and always know where they came from.
Document	.doc	Document files are a problem for older word processors and for word processors where macro protection has been disabled. Macros are a series of commands and instructions that you group together as a single command to accomplish a task automatically. Always make sure your macro protection (a feature which prevents auto-execution of macros) is turned on. If a document attempts to run a macro, don't let it unless you know what it is supposed to do. Some macros are important to the formatting or use of a document, but these should only be allowed when they come for a known source.
VB Script	.vbs	Visual Basic is a programming language in which scripts contain the code. You should never execute one of these files unless you are a programmer or you know the source of the file.
Batch File	.bat	This is the old DOS batch file, used for storing a series of commands that are executed together. Yes, they will still work under Windows and can do great harm. Always know what is inside of them before executing them. Before executing a batch file, use a text editor to examine the file or consult a professional.
Spreadsheet	.xls/.wks	Spreadsheets often contain macros and should be treated the same way as document files.

Safe hex 5: Treat infections promptly. It is essential to treat any sign of virus infection immediately. For specific information on combating a specific virus, consult one of the sites identified in "Safe Hex 1". If you're not sure what to do, hire a professional; after all you wouldn't try to treat a viral infection in your body unless you were a doctor or nurse. Treating just one computer is not the answer, either. Check all floppy disks, hard drives, self-made CDs, and any other removable media as well as your laptop and even your PDA. If you have a virus that self-replicates through e-mail, be honest and tell everyone in your mailing list about it. With a little warning they may be able to keep from getting infected.

Computers are a vital part of our everyday business activities, and their importance will only grow in the future. Don't be afraid of the Internet and the viruses that lurk there. Just practice "safe hex", and enjoy the fun and the benefits.

About the Author: Carroll Levison is an consultant specializing in IT Management with many credentials and certifications. He has over 30 years experience in the information technology industry as a network engineer, computer programmer, and computer operations specialist. He has extensive training and experience in computer security practices, has written several specialized virus simulation programs, and has been credited with being the first to discover and isolate one of the currently listed viruses.