

Learn-IT Newsletter for the month of May, 2005

## How to Prevent Catching the Common Code

by Mark Flores, MCP, MCSE

There are a lot of people with too much free time on their hands.

*One late evening, in the blue glow of a overheated monitor, someone of no particular importance squints approvingly and uploads his newly written code to a mass-mailing software application. Throughout the night his creation begins to travel the freeways of cyberspace, finding its way into thousands of awaiting in-boxes. The next morning at work, you turn on your computer and hear the familiar sound of new e-mail arriving. It's from your friend across town – the one who works for that new PR firm. "You have got to see this!" the title announces, so you open the message and with some disappointment, see that it only contains a few unintelligible characters. Oh well, on to the next message...*

*Behind the scenes, however, much more has just happened. When you opened the e-mail, a single pixel hidden on the screen executed an embedded piece of computer code, written just last night, and is now running in the background of your operating system. What is it doing? Who knows.*

At one time, it was common thought that only big companies needed to worry about computer viruses. But in recent years, these annoying, sometimes destructive creations have found their way into almost everyone's personal and workplace computers. According to a 2000 annual report by ICSA Labs (International Computer Security Association), more than 80% of survey respondents reported a median downtime of 21 hours with a direct cost of between \$10,000 (median) and \$120,000 (average) per year. In addition, according to the 2001 ICSA annual report, the number of virus infections has increased from an average of 3.75 per 1000 machines per month in 1996 to 110.5 per 1000 machines per month in 2001.

Here are 6 things that everyone should be doing to minimize the risk of getting a computer virus:

1. **Have an active anti-virus program running on your machine.** You can purchase anti-virus software at any computer or office supply store, or download them from the manufacturers' web site. Personal versions range in price from \$40.00 to \$60.00 and can also be purchased for corporate use with multiple licenses.
2. **Install security patches for your operating system, web browser and e-mail program.** Microsoft has a web site called Windows Update ([windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)) which will scan your system for any needed updates, also called *critical updates*.
3. **Do not open an e-mail attachment from someone you don't know without first scanning it for viruses.** Slow down when you are reading your e-mail. Don't absent-mindedly click on every attachment without first recognizing who sent it.
4. **Know the likely suspects.** Attachments with the extensions EXE, COM, SCR, BAT, DLL, VBS and CMD are highly suspicious. However, these files are perfectly normal in your existing operating system.
5. **Beware of risky download sources.** The creators of computer viruses don't need fancy software to spread their infections. All they need to do is post their files on publicly-accessible servers. FTP, IRC and popular 'peer-to-peer' music trading web sites are common targets.
6. **Don't expose yourself.** If you connect to the internet directly through your computer with cable or DSL, consider investing in a low-cost firewall device or router. These can be purchased at a local computer or office supply store for less than \$100.00.

### Relevant Terminology

**Back Door** – Originally, a 'back door' was part of a computer program that the creator could use to gain access to the application, even after the user had implemented their own security (remember the movie War Games?). A back door now refers to a piece of software that has been stealthily added to a computer's operating system (not by the original programmer) that allows a person to access the computer without the owner's knowledge.

**Macro** – Many programs use macros to automate common series of commands, such as Microsoft Word and Excel. Viruses can also be executed within a macro, so it is good practice to not accept a macro from an unknown source, and if there is any question, run a virus scan on the macro.

**Trojan Horse** – Although not technically a virus, a Trojan horse program disguises itself as something other than its intended purpose. For example, a screen saver attachment may work as expected, but also activates a secretly embedded virus or back door program.

**Worm** – Some viruses are activated when a certain program is run, but a worm is a virus that resides in the active memory of a computer and can therefore spread much easier through a network, e-mail or chat room.

The *Learn-IT* newsletter is published monthly by [Infinity Networking, Inc.](#) To subscribe to this newsletter and have it e-mailed to you automatically, send an email to [news@infinitycorp.com](mailto:news@infinitycorp.com). You can opt out of the newsletter at any time. Please feel free to forward this article to anyone who may find it of interest.