



July 2002

## Inside This Issue

1	"It'll Never Happen to Me"
1	Viruses
1	"Graffiti'd" Web Site
2	What Can I Do?
2	Be Careful of "Slammers"
2	Update your Anti-Virus!

Computer HelpLine, Inc.  
801 W. Street Rd, Suite 4  
Feasterville, PA 19053  
215-953-9930

[askus@computerhelpline.net](mailto:askus@computerhelpline.net)  
[www.computerhelpline.net](http://www.computerhelpline.net)

# Computer HelpLine Security News

## "It'll Never Happen To Me"

Hackers spend their time scanning the Internet, just looking for vulnerable computers. They're *not* looking just for the Fortune 500's computers; usually, they're looking for *any* computer they can break into, just to be able to say they did it. Suppose one of the holes they find is in your company?

Cyber criminals who are looking at a specific target organization (Microsoft, the Army, etc.) are especially interested in your small business's and personal computers. That's because they can use your computer to "relay" their attacks against the ultimate target through your computer. Why? When law enforcement backtracks where the attack came from, it'll look like it came from your computer, not the actual hacker's!

This newsletter will be dedicated to helping you make sure that you're not some hacker's next victim. Every issue, we will look at a different security topic and tell you what you can do to guard against it.



## Viruses

Every couple of months, it seems, the evening news is talking about the latest computer virus that's going to come along and put you out of business. There have been several in the recent past – Melissa and ILOVEYOU, and just recently, SirCam, Nimda, Code Red, and Klez. New viruses are being released (some might say "inflicted upon us") all the time. According to Symantec, makers of the popular Norton AntiVirus, 73 new viruses were released in just one week in May, 2002 (May 10 to May 17). A computer virus, in one sense, is like any other computer program: someone has written it to perform a specific task. The main difference

*Continued on page 2*

## "Graffiti'd" Web Site

Recently, a local township's Web site was hacked and "graffiti'd" (or defaced, as it's called in the computer industry). The material that the hackers put on the web site was definitely *not* family-friendly. Make sure nothing like this happens to your organization. Call us at 215-953-9930 to schedule a security assessment of your Web site and computer network.

between regular programs and viruses, though, is that viruses often are intended to do things to your computer that you don't want them to do – like erasing your files, crashing your computer, making your computer run slower, or in some way making your information and/or computer unavailable to you. Also unlike regular programs, viruses replicate, or duplicate themselves, and try to spread to other computers.

Virus experts say there are more kinds of malicious software than just viruses. “Trojan horses” are programs that appear to do one thing while actually doing another—think of the popular “Anna Kournikova” picture many people downloaded from the Internet. It did indeed have a picture with it, but it also did something else, completely different, that you don't know about.

“Worms” act like viruses, but they infect entire systems rather than individual files. The recently famous Code Red and Nimda viruses were actually worms.

## What Can I Do?

What can you, the average user, do to protect yourself against viruses? Practice safe computing, of course!

- Purchase and install an anti-virus program if you don't already have one. (For a list of popular anti-virus manufacturers and their Web sites, please see our Web Site, [www.computerhelpline.net](http://www.computerhelpline.net).)
- Be very careful about your incoming email (most viruses these days arrive by email). Make a habit of deleting emails that come from sources you don't know (without opening them first).
- Be especially careful of email attachments that do come from people you know, but that you aren't expecting to receive. Your friends and family may have sent you a virus without knowing that they did.
- Save all incoming attachments to your hard drive and scan them for viruses before opening them.
- Many viruses still spread on floppy disks. Be sure to scan any disk that you put in your computer with your anti-virus program.

## Be Careful Of “Slammers”

You may remember that a few years ago, long-distance telephone companies got into some legal trouble for switching consumers' long distance service without the consumers' knowledge or consent – a practice known as “slamming”. There are unconfirmed rumors of the same type of “slamming” going on in the domain-name registration business. For example: You have paid \$20 to Registrar A to register your domain name for one year. You expect to get a renewal notice from Registrar A near the end of that year. However, you get a renewal notice from Registrar B *before* you get the notice from Registrar A. Like most people, you don't pay attention to the detail of who your Internet registrar is, and you pay the bill, knowing that the end of the year is coming up. What you *don't* realize is that you have just authorized Registrar B to take your domain name from Registrar A, and you have probably paid a higher “renewal” fee and (possibly) a transfer fee as well. In reality, this doesn't affect the operation of your Web site and domain name – it only means you're paying more for that service than you have to. And *don't* say that you'll know the difference – especially not if Registrar B is a big, well-known company that “just might” be logically sending you a bill.

### *Update your Anti-Virus!*

Of course, if you bought an anti-virus program, or one came installed on your computer when you bought it, the anti-virus program will be able to protect you against viruses, right? The answer is: sort of. The program should protect you against all of the viruses that were known about when it shipped from the factory. Unfortunately, the program has no way of knowing about viruses that came out after it was shipped.

The manufacturers of anti-virus software spend a lot of resources keeping up with all of the new viruses, and coming out with cures for them as fast as possible. They're pretty good about it, too; most of the viruses have cures before they can cause trouble. All of the manufacturers release updates to their anti-virus programs on a regular basis, so that the anti-virus program on your computer can know about the viruses that came out after you got your anti-virus program. What you have to do is go the manufacturer's Web site and get the latest update. Or, if the anti-virus updates itself, you need to make sure that it is getting the updates.