A guide to pest control

Feeling insecure? Here are tips to prevent your files from infestation / **Simson L. Garfinkel**

PAUL GREENE'S DISCOVERY of a serious flaw in Microsoft's Internet Explorer has revived debate about security on the World Wide Web, or the lack thereof. The issue is serious because there are millions of dollars and reputations at stake as companies begin to conduct more business on the Internet and try to convince customers that the Web is a safe and reliable network.

What's so devastating about Greene's discovery is that the bug is so simple to use. Last year a group of graduate students at Princeton University's Secure Internet Programming group found similar problems in Netscape's Navigator program – bugs that allowed an attacker to build what was called "hostile Web pages." But the Princeton bugs were subtle and obscure. To use them, an attacker needed intimate understanding of the Java programming language as well as machine language code.

Greene's bug, in contrast, can be demonstrated with a single line of text on a Web page. With the bug, erasing all of the files in a computer's directory is as easy as typing "del *.*."

Microsoft is taking this discovery seriously. But mistakes like this will continue to happen. What worries me is that as the personal computer and the Internet become intertwined with our nation's financial system, we are going to increasingly see flaws, glitches, and bugs resulting in financial losses for hapless users.

In January, one of the first information warfare scams was uncovered involving a Web site called sexygirls.com, which promised free nude photographs of women. There was a catch: In order to see the pornography, the user first had to download a "special image viewer" and run it.

Users who downloaded the program soon discovered long-distance charges on their telephone bills. That's because the "image viewer" hung up the user's modem, disconnecting the user from his local Internet service provider, and made a long-distance phone call to Moldova, where the user's computer was reconnected to the Internet.

The scam worked because telephone companies in foreign countries receive a portion of the long-distance charges as a fee for terminating the call.

I pay my bills electronically using Checkfree. It's faster than sending checks and cheaper than postage. But last month, German's Chaos Computer Club demonstrated a program written in Visual Basic that could take over a copy of Quicken running under Windows 95 and initiate electronic funds transfers of its own. Even worse, the Chaos Club showed how the program could be incorporated into an ActiveX control and downloaded from a Web page, again using Internet Explorer. Microsoft reacted by issuing numerous press releases explaining how its "code signing" technology was supposed to prevent things like this from happening.

Unfortunately, code signing can't protect you from Greene's bug in Internet Explorer, or from programs like the sexy girls viewer that people willingly choose to run. The good news, though, is that you can protect yourself without severing your Internet connection or devoting yourself to the full-time pursuit of computer security.

Here are some simple things you can do:

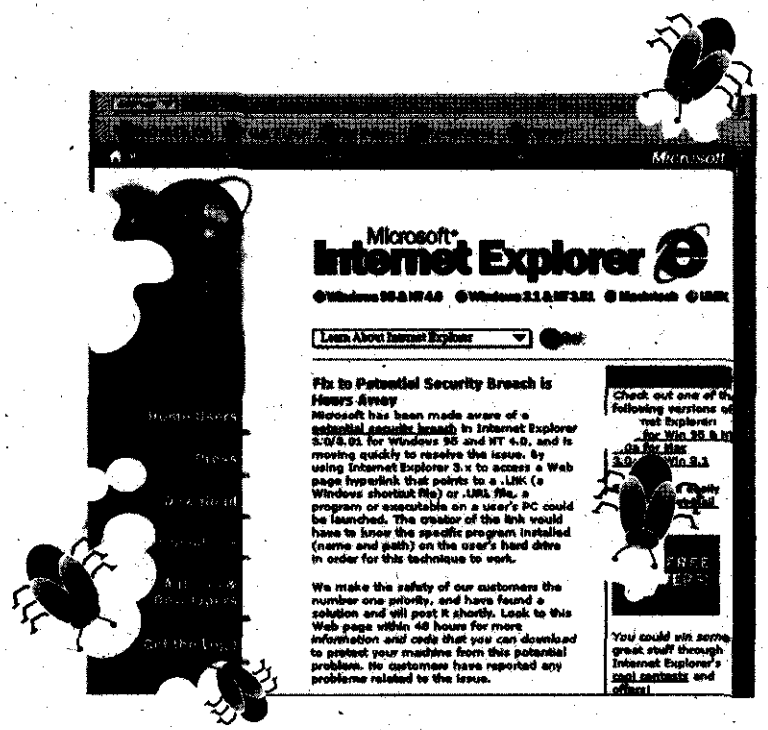
■ Be alert. Just as it's all but impossible to commit the perfect crime, it's equally hard to orchestrate an undetectable hack. If somebody or some program is messing with your computer, there is almost always some sort of tell-tale sign. Look for things that are unusual.

■ Be compulsive about backups. The best way to protect your computer is to back up the information it contains. For backups, I recommend getting a high-capacity, external tape drive, such as the Iomega Ditto EZ 3200 parallel. You want a drive that's high-capacity so you can make and keep many backups without worrying about running out of disks. You want the drive to be external so you can carry it around from computer to computer, and so that you can keep the drive (and your backup tapes) if you sell your computer to somebody else.

Iomega's ditto drive costs less than $300 and stores 3.2 gigabytes of information on a $35 cartridge.

I recommend against using a high-capacity external floppy drive, such as Iomega's Zip or Jazz. These drives barely store as much information as a hard drive and the media cost 5 to 50 times more than magnetic tapes.

■ Be attentive to your credit-card, bank, telephone, cable and utility statements. It is very difficult to steal money from somebody without leaving a paper trail. Part of that trail are the statements mailed to you every month. You should scan each statement and question every charge you don't understand or remember making. And you should keep your statements for at least two years, so that if you discover a problem, you can determine when it started.



The discovery of a potentially devastating bug has shaken the Internet.

Simson L. Garfinkel can be reached at plugged-in@simson.net.