SFGate.com www.sfgate.com Return to regular view

High-speed Net users sitting ducks for hackers
Open season on PCs without firewall protection

- Elizabeth Fernandez, Carrie Kirby, Chronicle Staff Writers

Sunday, August 26, 2001

It's the biggest computer threat you've probably never heard about.

Countless consumers are unwittingly making themselves targets of computer attacks by leaving their front doors wide open, exposed to the entire Internet world.

As more computer users convert to souped-up Internet access, as the ranks of the technically unsavvy grow, more are making themselves vulnerable to malicious hacking around the globe from powerful but invisible scanners.

Richard Lowe discovered earlier this month that he was a sitting duck. The Indianapolis businessman was stunned to get a call from the Bay Area, from an electronic Good Samaritan who said he was staring into Lowe's computer files and could have manipulated them at will.

At first, Lowe was angry that his privacy had been invaded. But he took the warning to heart, and did what many consumers have failed to do to their home computers: He turned off a function called file sharing and installed a firewall to thwart online trespassing.

"It ought to be automatic that no one can get into your computer unless you set it up for them to enter," Lowe said. "The onus should be on the DSL providers."

That's an issue being raised more often about broadband providers.

"When you get a high-speed Internet account, you get a packet of information on how to set up e-mail, how to build a Web page," said Jim Aspinwall, a Campbell computer consultant. "But nowhere does it say, 'Oh, by the way, you can be hacked and here are six steps to protect yourself.' "

High-speed connections -- last year the number of users doubled, with about 9 million households subscribing -- make break-ins easier because the computers are connected to the Internet around the clock via TV cable or phone lines.

Widening Internet use has triggered a race pitting electronic safety mechanisms against new spying devices, free and easy to download on the Web and capable of probing a computer's every nook and cranny.

While both sides try to outwit each other, many in the legal and computer community, as well as individual users like Lowe, increasingly maintain that broadband providers should shoulder more responsibility to educate and protect consumers.

"Service is being marketed, and the consumer has the expectation that accessing that service will not jeopardize the privacy and security of their computers," said David Kramer, a Palo Alto Internet attorney.

"It is not an unreasonable expectation. When you buy telephone service, you have the expectation that the risk of someone listening in is pretty limited. Awareness of the security risk in the general public is pretty low. It would be great to see DSL providers alerting people to the potential risk."

ILLEGAL SCANNING

Illegal scanning can occur without the knowledge of computer owners, until they discover their personal data have been tampered with.

Yet consumers are, in effect, holding out welcome mats by using the file-sharing feature on operating systems that are designed to allow users to trade documents with others on a private network. Many users fail to realize that file sharing also enables the entire Internet to browse their computers, leaving them bare to attacks from scanners or viruses probing for open drives.

"People are just starting to exploit this problem," said Marc Perkel of the Electronic Frontier Foundation, a San Francisco organization that protects free speech online.

Although security experts have long recognized the risks, even those who work in the industry are not exempt from exposing themselves to online marauders.

"Guys at work had been talking to me about security for my home computer, but I kept thinking 'Yeah, I'm safe,' " said San Jose resident Steve Johnson, who works as a designer at Adobe Systems. "It's like your mom telling you to put on your jacket. You don't really listen until you get sick. You hear about big companies getting hit, but you say to yourself, 'I'm Joe Schmo, no one would waste their time hacking into my computer at home.' "

Months after Johnson installed DSL, he "snapped out of my Type A maleness" and purchased a firewall system.

"You would never leave your front door unlocked at night, but you don't think of doing the same thing at the other end of a computer," Johnson said.

In Los Angeles, a class action suit alleges that Pacific Bell, the state's biggest DSL provider, falsely advertised the service as secure and failed to inform consumers to protect their computers from unauthorized intrusions.

'NAKED TO THE UNIVERSE'

"I thought I was pretty sophisticated about computers, but I had no idea I was sitting out there totally naked to the universe," said Nathan Hoffman, a Woodland Hills attorney who filed the suit after purchasing DSL two years ago for his home office.

"I noticed files were missing, things weren't right," Hoffman said. "My machine was ripe for taking. Many other people don't know how to protect themselves. They think their computers are secure because they have virus software. That is just not so."

A Pacific Bell spokesman declined comment on the lawsuit, but said when technicians install DSL, file sharing is left as the customer set it.

However, the company's Web site and technical support staff advise against file sharing if customers don't need it for a home network, said spokesman Fletcher Cook.

"As far as telling people they have to turn this off or doing it for them, it's really against our policy," he said. "I think we're doing a lot as far as . . . arming consumers with the information they need to make the appropriate decisions. It's up to them . . . what they want to put on their computer and how they want to protect themselves."

When a new computer comes out of the box with Windows installed, file sharing is turned off by default. But there are a variety of ways people might turn it on, security experts say.

Users can purposely enable file sharing to connect several computers together at home, but be unaware their computers are also open to the whole Internet. Or a user might bring a computer home from work, not understanding that the computer is configured to operate in a network, behind a firewall.

CALL TO PROVIDERS

"I think both (Microsoft and broadband providers) have some level of responsibility to solve the problem," said Richard Smith, chief technology officer with the Privacy Foundation in Denver.

"A lot of people make the mistake of leaving sharing on. It's a pretty easy mistake to make. I did it myself. I left my hard drive open for about a month when I got DSL. When I discovered it, I thought, 'Oh, my God, I'm wide open.' "

Los Angeles security expert Steve Gibson created a tool two years ago that allows computer users to check their own systems for rogue scanners. Of more than 9 million visitors who checked their systems on the site, almost 2 million had exposed directories, Gibson said.

Since discovering earlier this month that he could download free scanning software so simple to operate "a chimpanzee with no arms could do it," Burlingame computer consultant Michael Chukov has made it his personal crusade to alert users to take safety precautions.

In a few days, Chukov found 7,811 open computers in the Bay Area and across the country. There on his screen were confidential files belonging to lawyers, accountants, businesses. Employment records, Social Security numbers, all of them were easy pickings for electronic tampering.

The self-styled Robin Hood of hacking was so infuriated he contacted many of the people whose computers he had invaded to advise them to safeguard their files.

His thanks? Not much.

Most were furious. And embarrassed.

"I had to try to do something," Chukov said, undaunted. "You don't go by a house on fire and keep driving."

HOW TO PROTECT YOURSELF

To check if file sharing is turned on, look at the folder icons in your Windows Exploring screen. If a folder is open for sharing, it will have a picture of a hand on it.

To test for common vulnerabilities, such as file sharing, go to www.grc.com and use the free program, Shields Up.

If you don't have a home network, turn off file sharing. For instructions go to: www.mikeshardware.com/report_hacked.html and click on ""Turn Off Your File Sharing."

If you have a home network, make sure you use passwords whenever sharing drives.

Install a firewall. The Web site About.com has advice on how to pick one at .netsecurity.about.com/mbody.htm.

Upgrading your operating system might help. Microsoft says its new Windows XP will make it easier for users to avoid inadvertent file sharing. But it won't be clear whether the new operating system will actually be safer until after its Oct. 25 release.

UNDERSTANDING YOUR COMPUTER'S VULNERABILITY

Q: What is file sharing?

A: If you are using Windows, file sharing is an option that's built into your system. If you activate it, other computer users … potentially everyone on the Internet … can see and change files on your computer. Someone could even use file sharing to add dangerous programs to your hard drive. If you use file sharing, it's recommended that you limit access to your computer by setting a password and using a firewall.

Q: Who should worry about this?

A: Anyone who uses the Internet could be intruded upon via file sharing. It can happen if you have a dial-up connection to the Internet, but people using broadband access like DSL or cable modems are more likely to be affected because their computers are generally connected all the time. Most of the tips found here are for Windows users, but users of Macintoshes and other operating systems may also be at risk.

Q: If I turn off file sharing, am I safe from malicious hackers?

A: Turning off file sharing is like locking your front door … no one can get in through that entrance. But hackers might be able to find other entrances to your computer. New ways to break into computers via the Internet are discovered all the time. To prevent this, it's best to use a firewall and to make sure your operating system has the latest "patches" to block intrusion. Windows users can update their systems at windowsupdate.microsoft.com.

Q: What is a firewall?

A: A firewall is a barrier that you erect between your home computer or network and the Internet as a whole. Firewalls are available in the form of software or hardware, and range in price from free to about $180.

Q: Are you safe from intrusion if you turn your computer or modem off when you're not using it?

A: No one can break into your computer while it or the modem is turned off, but if you do not take the suggested precautions, someone could still get into your computer as soon as you turn it on.

Q: How do I know if someone is intruding into my computer?

A: Some firewall packages tell you when someone has broken into your computer, or is trying to. For details about some popular firewall products, visit the Web site .netsecurity.about.com.

Q: I have to enter several passwords to use my computer and various programs on it. Won't that prevent intruders from seeing my files?

A: You must specifically set a password on the Windows file sharing function. You will be prompted to set the password while you are turning on the file sharing function. Other passwords on your computer may not prevent people from using file sharing to access your hard drive.

E-mail the writers at efernandez@sfchronicle.com and ckirby@sfchronicle.com.

Page A - 1
URL: http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2001/08/26/MN209383.DTL