



Archive

from the July 29, 1999 edition

Logged on all the time has its dangers

James Turner

BOSTON— Internet users fed up with the relatively low speed of dial-up connections may consider cable modems and other high-speed connections a blessing. But along with the high speed and constant connectivity (the Internet dial tone is always on) comes some increased security risk and a requirement for greater diligence

Most of the risk comes from the persistence of the connection. Because dial-up connections are constantly made and broken, the Internet provider (IP) address of your computer constantly changes. This means that someone trying to break into your system has a limited amount of time to probe your defenses before the connection is broken and a new numerical configuration is created. Conversely, cable modem connections persist for days or weeks with the same IP address assigned to your computer. This gives a potential intruder lots of time to try out his or her bag of tools against your system because only one unchanging numerical configuration is in use.

In addition, many cable modem systems are designed so that all the computers on a local loop of the system (like a telephone party line) appear to be on one big local-area network (LAN), a short-distance network used to link a group of computers together within a building.

Operating systems like Microsoft Windows may be inadvertently broadcasting their presence to everyone else on the cable system. Some cable companies, like Colorado-based MediaOne, have started filtering out this possibility. This shields your system from having its local file systems exposed to the outside world.

Still, there are some simple steps that will increase your protection.

*If you use a system that stores software from other systems to share your connection, you have some special concerns. Improperly configured, this connection could allow outside users a gateway to your computer. The vendor should have information on its Web page about how to guard against this.

In general, if you have a LAN set up in your home, you should take the time to learn the basics of network security. You may even want to learn something about firewalls, software designed to protect your LAN from unauthorized access from outside your system.

*Don't run Web or file transfer servers on your computer unless you are absolutely sure you understand the security configuration involved.

*Use a virus scanner to guard against software that allows others to gain control of your computer via the Internet.

*Don't open e-mail attachments you don't recognize. Don't run software if you're unsure of the source.

*Check on your service-provider's Web pages for additional recommendations on how you can configure your computer to protect yourself.

[Subscribe to *The Christian Science Monitor* weekly edition](#)



LINKS OF INTEREST

[Chinese toy recalls show need for stringent quality control](#)

[Crisis summit aims to save Iraq's Maliki](#)

[South African AIDS activists criticize firing of Madlala-Routledge](#)

[Hizbullah marks Lebanon war anniversary with pomp and piety](#)

[Democrats gain among US voters, but support is soft](#)

[Like the look of a traditional newspaper? Try the Monitor's Treeless Edition](#)

MOST VIEWED

1. [Obama wins over a Montana crowd on healthcare](#)
2. [The war on drugs needs a timeout](#)
3. [Truck bomb signals trouble on Russia's southern flank](#)
4. [Oops, he did it again: Jamaica's Usain Bolt sets new world record](#)
5. [Firefighters make progress against Santa Cruz fire](#)
6. [Riot shows difficulty of desegregating California prisons](#)
7. [As a CIA spy, I saw in Iran what the West cannot ignore](#)
8. [Review: 'District 9'](#)
9. [Obama's health ideas elicit support, skepticism in Colorado](#)
10. [Ahmadinejad blames West for fomenting Iran unrest](#)