Can Osama See Your Data?

By Daniel K. Kehoe

To be honest, it's more of a rhetorical question than a practical one, but it brings to mind the concern about the sensitive actuarial data sitting on your computer. Because the Internet is largely flat by design, data that is viewable by someone else in your office could also be viewable by Osama Bin Laden and anyone else who is connected to the Internet.

That ought to make you take the time to check your own personal computer for security leaks.

The Right Operating System

First, if you are a Windows user, you should be using Windows XP or Windows 2000 (or 2003 if it is a server). Older versions like 95, 98 and ME are just too problematic to secure. Most of Microsoft's attention to security issues is aimed at their current home and business offerings.

Even if you have a current operating system, the file system could be a problem. The newer NTFS (NT File System) is more secure than the old FAT32 (File Allocation Table) system. To see which you have, open up My Computer and right-click your C drive and choose Properties. It is possible to convert FAT32 disks to NTFS in place.

Windows XP Professional is a better choice for actuarial users than XP Home Edition because it offers EFS (Encrypting File System) and stronger user authentication methods. Most business class computers tend to ship with this version, but you can also upgrade to Pro for about $170.

Look For Holes

A handy tool for checking your system's security level is available as a free download from Microsoft. The Microsoft Baseline Security Analyzer will look at your system, warn you about a whole host of security problems, and make suggestions to fix them. It's not perfect, but it catches most of the obvious security problems. You can find it here: http://www.microsoft.com/technet/security/tools/mbsahome.mspx.

There are some really good Web sites that go into detail about security tips and tricks. Using a search engine is the best way to find sites that can help you shut off unnecessary software modules that could lead to people breaking into your computer. A place to start is: http://antivirus.about.com/od/securitytips/.

You can set Outlook Express to read all your email messages in plain text (turn off the ability to read HTML by selecting Tools → Options → Security → Change Automatic Download Settings, and check Block images and other external content in HTML e-mail). Plain text can't hurt your PC, whereas HTML components could be virus-laden or could redirect you to websites. Also, these HTML components embedded in e-mails can

sometimes collect information about you and your computer that could be used to break in.

To keep nosy people out of your network, you need a hardware firewall, period. The software firewall that comes with XP Service Pack 2 is nice, but keeping people from even getting to your computer is better. Most wireless and cable routers come with firewalls built in. If you have a single computer connected into a cable or DSL modem directly attached to the internet, you are vulnerable.

Google Yourself

You'd be surprised to find what information exists about you on the internet. Use Google or your favorite web search engine and type in your name in a couple of formats. You'll find conference attendance listings (with e-mail addresses), mentions about you in online newsletters, and other mentions about you. Even if you ask the webpage owner to take your data offline, these pages hang around in search engine caches for months.

These caches are also a sneaky way to see postings in member-only conferences. In Google, for instance, your search might bring up a link to a posting with your name mentioned in it, but when you click on the link, you get a page telling you that only members can view the postings. Instead, click on the "Cached" link to the stored version of the page, and suddenly you're there, reading a copy of the post inside the conference.

Lost in the Crowd

Oddly, you are practically invisible because there are so many other targets out there. It's why your car is rarely broken into when there are so many other choices parked at the mall around you. But anyone looking specifically for you and the data your customers have entrusted to you now has the power of the Internet to start his search.

There isn't space to tell you how to fix your security issues, but at least you can be aware of them. Browse some the security websites and tighten up your security or call in an expert. Keep Osama, and everyone else, out of your data.

Daniel K. Kehoe is president of Bigfoot Labs in Connecticut. He has over 27 years experience in the computer industry in technical and marketing roles, most recently with Compaq Computer Corporation.