BY JOSEPH S. EASTERN, M.D.

MANAGING YOUR DERMATOLOGY PRACTICE

Prevent Computer Abuse

As I discussed last month, the rapid evolution of electronic medical records and electronic claims filing has greatly increased the role of computers in our offices, and this trend will continue for the foreseeable future, largely because the federal government has decreed that it will happen whether we like it or not.

But, of course, with progress comes new problems. As computers become more ubiquitous, computer abuse will become a larger and larger threat.

It is already a major issue in the general business world. Here are some statistics from a recent industry survey:

► Two-thirds of employees with Internet access admit to using it for personal diversion during working hours.

► At work, 30%-40% of Internet time is spent on non–work-related browsing, and 60% of all online purchases are made during working hours.

► Seventy percent of all Internet porn traffic occurs during the 9-5 workday.

In short, up to 40% of lost productivity can now be blamed on computer abuse.

But lost productivity isn't the only problem. Unauthorized Internet access increases vulnerability to viruses, worms, and trojans, which can shut down your network.

On top of that, an estimated 80% of computer crime, such as embezzlement and theft of intellectual property, is done by "insiders"—employees working within the victimized companies, on company time.

"Outsiders" can be a problem too. If your office runs an unsecured wireless network, anyone with even a marginal command of network mechanics can easily gain access to your practice finances, your patients' medical records—anything running on your computers.

If you have an application service provider (ASP) system, where your medical records are stored electronically on an offsite server, such potential security breaches are an even bigger issue, for both patient confidentiality and general efficiency. So it behooves you to pay close attention to how your computer network is set up and how your computers are used on your time.

Start with computer monitoring software. Several reasonably-priced programs are available. They automatically and discreetly record everything done on a computer, including Internet activity, chat rooms, instant messages, and Web sites.

Examples include Snapshot Spy (www.snapshotspy.com), Spector Pro (www.spectorsoft.com), and SoftProbe Analyzer (www.softprobe.com). (As always, I have no financial interest in any of the companies or products I discuss.)

Monitoring software runs quietly in the background and cannot be detected by users, but I strongly advise informing your employees that their computer use is being monitored for their safety as well as yours.

Protecting your network from unauthorized access and signal diversion is a more complicated issue. For starters, don't use the default system ID, since any hacker can find that in the user's manual. Change it to something unique—not your birthday or your pet's name. Disable "identifier broadcasting," which announces to the world that you have a wireless connection. Enable any encryption supplied with your network, and get more if you need it. (See below.) Configure your router to allow only incoming or outgoing traffic that you have approved. Depending on the complexity of your network, you may need more sophisticated protection, such as AirDefense (www.airdefense.net), CRYPTOCard (www.cryptocard.com), or LucidLink (www.lucidlink.com).

It goes without saying that all of your computers, including private ones, need personal firewall software such as Zone Alarm Pro (www.zonelabs.com) and good antivirus, antispyware, and antiadware protection, updated frequently. And change your administrator password often—at a minimum, every time an employee leaves your employ for any reason. ■

DR. EASTERN *practices dermatology and dermatologic surgery in Belleville, N.J. To respond to this column, write Dr. Eastern at our editorial offices or e-mail him at sknews@elsevier.com.*