Wired to the World

by *Ralph Lee Scott*

Physical Security

A very important way you can enhance the security of your computer system is to provide additional layers of physical security. This means doing some obvious things such as not leaving your laptop on a seat in the airport while you go to get another latte, and locking your office door when you are out of the office, even for just a few moments. Keeping servers under lock and key and not allowing physical access to the room except to those who must have access is also important.

Using a BIOS password provides some protection, but a determined hacker can take the computer apart and remove the battery, thus destroying the BIOS password. Some people like to use bicycle-type laptop computer locks. You need to be sure that the end of the cable is attached to something secure, since attaching the cable to a wooden desk, for example, is probably not going to stop a determined thief.

An additional step you can take to protect your computer is to brand your hard drive with a program like Brandit (available from: http://www.dmares.com/maresware/brandit1.htm). Brandit places identifying information on your hard drive that cannot be erased by reformatting the drive. If your computer is recovered, you can activate a key that will reveal your original ownership of the system.

Other simple ideas can help, such as not having computers in locations where passwords can be seen as they are typed. Make sure that only authorized people have access to the office area where your computer is stored. Always lock doors when the room is unattended. Changing passwords often and making passwords that are a combination of letters, numbers, and special characters is important. If your computer has a lock system, use it. In fact, some libraries put theft detection strips in laptops so that the alarm will ring when the computer leaves the building.

Having an accurate inventory of your equipment is also an important part of physical security. Be sure to erase from paper records any log-on IDs and passwords. This will prevent hackers from "dumpster diving" for computer security information. This means also keeping electronic records secure: lock up disk and removable storage drives that might have password and ID information written on them. Keeping public computers in a heavily used space with a clear view for supervision can also help. If you hide the computer in the stacks, it is an invitation to someone interested in destroying equipment.

Check your security logs frequently for usual activity: deleted entries, incomplete or short logs, logs with incorrect permissions or timestamps (like January 1st when the building was locked up), or odd records of rebooting or startups. Generally, if someone gets into your computer when you are not present, he/she will leave a log of his/her use in the event log. Simple tasks such as rebooting are logged into the event logs.

Check these logs for unauthorized times of access. For example, if you lock up your office laptop everyday at 5:15 p.m. and you notice that the event log shows that the machine is turned on at 3 a.m. several nights a week, this is a clue that someone is using your machine when you are not at work. If you are unfamiliar with Windows event logs, just click on the start pull down menu and select "Help." Then type in "event viewer-finding" in the index and "Help" will show you how to access these logs. There are actually three logs in Windows: Application, Security, and System. Check all three for unscheduled use of your computer.

Having taken steps to prevent physical access to computers, you also need to prevent physical access to the information in the computers. This can be done by encryption schemes that scramble the information on the disk. One of the widest used is CodedDrag (http://www.fim.uni-linz.ac.at/codeddrag/codedrag.htm). This is a modest program that costs only $30.

For the ultimate in personal computer protection, visit http://www.uoe.dk/csworld/security-.html , where you can read about an enterprising Dane's instructions for encasing a personal computer in 110 pounds of concrete. Unfortunately, in an addendum to the story, the 110-pound computer was carted off and dumped in a nearby ditch!

This article concludes a four-part series on computer security, including the following topics: Spyware, Anti-Virus software, Firewalls, and Physical Security.