Top Ten Laptop Computer Security Recommendations

1. Use visual deterrents.

A cable lock or other locking mechanism can act as a deterrent to would-be criminals. Although they can be ripped off the plastic exterior of a laptop with a strong tug, they do force some criminals to think twice before taking the risk.

2. Avoid leaving unsecured laptops unattended.

Lock them in cupboards, laptop carts or other secure facilities when not in use. If they must be left in a vehicle, they should be covered up or locked in the trunk.

3. Keep laptops inconspicuous.

Laptops should always be carried in inconspicuous carrying cases, such as backpacks or tote bags, instead of tell-tale laptop bags.

4. Use complex passwords and change them regularly.

Don’t use simple passwords that can be guessed easily. Always use a combination of numbers and letters and never leave your password in obvious places on or near the computer. As well, password-protect your screensaver to avoid unwanted access to your computer if you’ve stepped away.

5. Leverage antivirus software, encryption solutions, anti-spyware and firewalls.

Prevent unauthorized access and spyware from invading your computer and protect valuable information with data encryption software. Make sure your systems are properly installed and kept up-to-date.

6. Back-up valuable data on a scheduled basis.

Data back-up needs to happen as frequently as possible to minimize the risk to organizations in the event of theft or loss. The information or ‘knowledge’ that is stored on the computer is more valuable than the computer itself.

7. Understand the dangers of pirated software and file sharing.

Both piracy and over-deployment of purchased licenses can lead to significant lawsuits or other financial penalties. Not only is it illegal, but pirated software can increase susceptibility to viruses, trojans and other attacks.

8. Stay informed.

Continue to educate yourself on the tools and techniques used today by cyber criminals as well as the latest scams and other security risks to company data.

9. Use asset tracking and recovery software.

Laptop recovery tools are highly effective, especially those based in the BIOS of computers, such as Computrace LoJack for Laptops by Absolute Software. They not only recover the hardware, but stop the root cause of internal theft by catching the thieves. And regulatory compliance today requires that companies know not only what is on a computer, but where it is, and who is using it.

10. Invest in advanced data protection.

Leverage advanced data protection technology to remotely wipe sensitive information in the event that your computer is lost, stolen or nearing the end of its lifecycle.