Case Study: Safeguard your Personal Computer

In the aftermath of the September 11 terrorist attacks, businesses and home PC users are consciously thinking more about protecting themselves as well as existing data obtained like never before. Despite the types of physical attacks demonstrated on September 11, PC's are constantly under some type of attack. In a nutshell, a personal computer connected to the Internet without a firewall can be hijacked in just a few minutes by automated hacker "Bots". The only way to make your computer 100% secure is to turn it off, or disconnect it from the Internet. The real issue is how to make your computer 99% secure when it is connected. Not having protection is like leaving your car running with the doors unlocked, windows down, and the keys in it, which a thief might interpret as "please steal me". Stated another way, when was the last time you handed a stranger your wallet and encouraged them to take your social security card, driver's license, cash and credit cards? Locking a car, using a "club" or installing a security system makes stealing a car more difficult. Internet security and privacy products provide adequate protection by making it difficult for "outlaws" to take control of your computer and rip you off.

The bottom line, at a minimum, is any computer connected to the Internet needs to have all current patches to its operating system and browser installed as well as personal firewall, antivirus and anti-spyware software. A more complete solution is taking a layered approach to protect your security and privacy as follows:

- **First line of defense** -- Choose an **Internet service provider** and/or an **email service** that offers online (server side) virus and spam email filters.
- **Second line of defense** -- Install a **wired** or **wireless** hardware router with a built in firewall between your modem and your computer or network. Also consider using a **broadband gateway** offering a combination of hardware and security software.
- **Third line of defense** -- Use a **security software suite** or a collection of individual software products including, at a minimum, **personal firewall, anti-spyware,** and **anti-virus** products. Also consider using **anti-Trojan, anti-spam, anti-phishing,** and **privacy** software. Please note that cost is not an issue since there is good **security freeware** available.

Important Tips

- Update and **tighten** Windows before installing new security software.
- To avoid conflicts, do not use two software firewalls or two anti-virus products at the same time. Completely uninstall one before installing another.
- You can and should use a hardware firewall and a software firewall at the same time.
- A security software suite or broadband gateway may be supplemented with individual products as needed to add or strengthen a feature. Also, if you are given the option, do not install features that you do not need or will not use.
- After installing any security software, **immediately** check for updates at the vendor's website.
- After installing a firewall, use an online **testing** service to make sure that it is working correctly.