

# How to Secure Your Most Important Asset

By Matt Banks



Many go through their day preparing memos, status reports, plans and presentations on their desktops, printing to shared printers, backing up data on their servers, surfing the Web on laptops and sending e-mails from their BlackBerries and Pocket PCs. What would you and your business do if one or all of these went down? How long could you conduct business without your computer system? Most businesses would not make it through a normal work day without theirs. Chances are your business is no different.

Are you prepared for a mass problem that could shut down operations? The solution is to prevent them from happening. Maintenance and updates are vital to keeping your computer system running smoothly and securely.

Your computer needs maintenance on regular intervals just as your car needs its oil changed and tires rotated. People are trained to take care of their cars, but many forget, or don't even know, that they need to care for their computer system as well. Many feel their car is deserving of regular care because of the high cost to purchase it. One computer may be less expensive when compared to a vehicle, but think of the information they store for your business and customers, the power and speed they give your employees, and the revenue they help generate.

Most business owners don't believe they're a target, nor do they know when they've become one. The fact is anyone or any business can be a target. Based on expert tests, the average unprotected Windows computer with the most common security holes will be hacked within 20 minutes. Even secured computers will be scanned for vulnerabilities dozens of times each day.

Securing your computer can be done by following a few simple steps and investing as little as a few minutes each day.

Your first step in computer maintenance and security is to enable a firewall on each computer. Even if you have a dedicated corporate firewall, it's a good security precaution to have a simple software firewall enabled, such as Windows Firewall, in case of network intrusion.

Perform Windows and Office updates weekly. These provide fixes for security holes and performance increases for Microsoft Windows and Office software.

Antivirus scans should be performed at least once per week. Most new computers come with antivirus software already installed, but it requires the regular updates to tell the program how to identify the latest threats.

Browse the Internet long enough and your PC will inevitably be infested with some form of spyware or adware. These malicious programs can slow your computer and Internet connection and snoop on your Web browsing activities. Antivirus and antispyware programs

should be run at least once a week to check for updates.

Never click indiscriminate links. They can lead to many types of spyware, such as a keylogger, as well as viruses. Phishing e-mails are also becoming very sophisticated.

Servers need just as much protection as each computer on your network. A firewall will control who can access your server and what data can be sent out. To provide the highest level of security, a network security appliance can be added to provide a fully customizable, dedicated hardware firewall and content filtering system.

Windows Update and Server Application Updates should be run weekly on your server as well as scheduled antivirus updates and scans.

Each workstation and server should be set up with a password of at least eight characters, including numbers and letters, preferably both lowercase and uppercase, or a non-alphanumeric character.

The importance of information backup can not be stressed enough. It is a daily must. Always backup to external media, such as CDs, DVDs or tape drives. Even if you have a dedicated NAS (network attached storage) or SAN (storage area network), you need to have an off-site backup in case of a catastrophic system failure.

All this information may sound overwhelming and that is why many businesses choose to overlook it. It seems easier to forget about it now and deal with the problem down the road. You can't do that with your business and all of its vital information. Think of what information and work time you have to lose. It is much easier and more cost effective to conduct regular maintenance than it is to repair a system failure when it happens. If you are not taking care of you computer and network, then chances are they have been infected and you don't even know.

*Banks is President of Kernel Computer Services. For more information, visit [www.kernelcomp.com](http://www.kernelcomp.com) or call (518) 774-0306. ■*



Custom-made: *Unique, one of a kind, like no other*

**THATCHER BROOK  
MILLWORK & DOOR**

75 MOHICAN ST. GLENS FALLS, NY 12801  
518-761-0568

Manufacturing Quality Custom Millwork –  
Cabinets, Moldings, Countertops and Doors. **AWI**