

**If your computer can connect to the Internet.....  
people from the Internet can connect to your computer.**

## **10 easy steps to increase security without a heavy price tag**

### **1. Consider the right Operating System**

Windows 9x (95, 98, ME) do not have ANY security and should not be used in a business environment.

Windows NT is quite secure as long as the file format is NTFS. Most companies have upgraded to Windows 2000 or Windows XP

Windows 2000 is still widely in use. It offers file-level security and encryption.

Windows XP Professional with SP2 has now been widely accepted by the industry. There are still some issues to “tie it down” but the general feel is that this OS is here to stay and more and more companies are integrating XP. The XP Home Edition is not suitable for Networking.

If you know a lot about computers and feel adventurous, Linux is an alternative in certain areas.

### **2. Only install what you really need**

With the default installation of all operating systems, a wide range of services are installed. Most of these services are not needed and are sitting on your computer, waiting to be compromised.

Do not install anything that isn't required. After the installation is finished, check which services are running and disable what you don't use. (The Internet Information Service is a very good example)

**How to:** Control Panel/System/Services or with 2000/XP: right-click “My Computer”, select “Manage”, select “Services”. Double-click on an unused service and select “Disable”.

### **3. Protect your Hard Drive**

Implement secure access by removing the “Everyone” group from the access list and replace it by either “Authenticated Users” or specific user accounts.

**How to:** Open Windows Explorer, right-click on the C drive, select “Properties”, select “Security”, highlight “Everyone”, delete, select “Authenticated Users” or a specific user. Repeat these steps for all other drives.

### **4. Install a good Virus Protecting Software – AND update regularly!**

Symantec and Trend Micro are among the most trusted programs. McAfee has lately been questioned by many consultants.

Wherever possible, a centralized system (Enterprise Version) is the better way to go. The slightly higher purchase price will be recovered very quickly through lower maintenance cost and increased reliability.

- 5. Take Cover - Use Routers, Firewalls and Proxy Servers**  
Hiding behind some kind of barrier increases security substantially. It is much more difficult to attack your computer when it is not directly accessible from the Internet. Routers, Firewalls and Proxy Servers channel the traffic from and to your computer. For about \$100.00 a small office can be secured.

**Tip:** Make sure that all unused protocols are disabled. Normally only HTTP (port 80) and SMTP (port 25) are needed. If you use your ISPs email, POP3 (port 110) has to be open as well.
- 6. Be aware of Spy Ware**  
Spy Ware are programs that examine your hard drives and mail selected items to their creator or function as “Key Logging” utility, transmitting every key stroke you perform on your keyboard. Antivirus programs normally don’t detect this kind of intrusion. Only monitoring your network traffic will tell you that spy ware is active on your computer. Several products have been put on the market over the last year that will analyze the network traffic against a database to detect known patterns. Pest Control is one of the better ones that allow control without requiring detailed IT knowledge to use it.
- 7. How secure are you?**  
Knowing the holes is the only way to plug them. Test your system and find out where the holes are. Several companies offer a free service. “Shields Up” is one of the best. You can connect to [www.grc.com](http://www.grc.com) (Gibson Research) and test your computer. You will get instant results. Don’t forget to do the “Port Scan” as well.
- 8. Don’t leave you back door open - Inside Security**  
One of the most common mistakes in the home office and in the small business environment is the lack of physical protection of your electronic assets. If you don’t use any passwords or use easily guessed passwords, anybody that can get to your computer, can steal your information.  
And here is another one: The best password doesn’t help if you don’t log off the computer before you leave the office.

Whenever possible, servers should be locked up in a separate room or even a closet. If they are properly configured, it is much harder to break into them over the network than being able to sit in front of them.
- 9. The other Enemy – Hardware and Software Failure**  
After taking all precaution against intruders, people very often forget about the number one culprit when it comes to loosing electronic assets: Hardware and Software failure. Several studies have shown that 85% of companies that loose their data will not recover or file for bankruptcy within the first 6 months.

Backing up your data on a daily basis is relatively easy and doesn’t need to cost a lot of money. Free tools are available within the operating system and hard drives are not expensive anymore.

**Spend a few minutes of your work day to protect your life’s work.**
- 10. Fires do happen**  
Last but not least, make sure you take periodically a copy of your data to a different location. Depending on the amount of data, tapes or even CDs will do the trick. There are also companies around that offer remote storage.