

## Protecting Your Laptop with 12 Simple Laptop Security Tips

While computer operating systems today are much more secure than just two years ago, there is still some user management necessary. These operating systems, such as Microsoft Windows XP are becoming more and more “user friendly” from a security standpoint. Many potential security problems are locked down by default and the user generally does not need to be concerned with implementing them.

However, computer security (“cyber-security”), in general, is still somewhat reactive. Good examples of being reactive are the Anti-Virus products on the market today, for example Norton Utilities by Symantec. While they try to anticipate new types of attacks, they still can not effectively predict specific attacks, because the creators of such attacks are effectively on the “offensive.”

Most laptop computers today use Microsoft’s Windows XP, SP2 as the operating system. This release has some of the best security features currently available for a computer, but they need to be checked or in some cases implemented by the user. A good example of this is an anti-virus product installed on your laptop. Not only does the Anti-virus software need to be enabled, but the Microsoft XP settings may need to be changed to accommodate the anti-virus changes. It is the user’s responsibility to make sure this protection is enabled.

These checklists outline the steps you should take to reach a baseline of security with Windows XP Home Edition and Windows XP Professional computers, either on their own or as part of a Windows NT or Windows 2000 domain. Additional information about these checklists can be found on the Microsoft Website. Just search on the Microsoft site using the term “security.”

**Important:** The purpose of these checklists is to give instructions for configuring a baseline level of security on Windows XP computers. This guide does not provide a complete list of all security features provided in Windows XP or how to use them. A complete list of new security features available in Windows XP is available on the [Microsoft Web site](#).

### Windows XP Professional Configuration - 12 Steps

1. Verify that all disk partitions are formatted with NTFS
2. Protect file shares
3. Use Internet Connection sharing for shared Internet connections
4. Enable Internet Connection Firewall
5. Use software restriction policies

6. Use account passwords
7. Disable unnecessary services
8. Disable or delete unnecessary accounts
9. Make sure the Guest account is disabled
10. Set stronger password policies
11. Set account lockout policy
12. Install antivirus software, antishareware software and updates

These security tips are suggested by Microsoft to provide a baseline level of security for your computer. Additional security steps that are very important to protect your laptop and desktop computers include:

- Keep your data safe and backed up
- Use the Internet safely
- Protect your networks and servers, especially when wireless access points are used

Microsoft has a tool called the Baseline Security Analyzer that is excellent. It helps detect security threats and is a must have tool for anyone interested in security for a laptop, desktop or computer network.

## **Laptop Theft**

Another very real security threat to your laptop is theft. According to Safeware Insurance, “387,000 laptops were stolen in the US in the year 2000 - versus 319,000 in 1999.” The FBI notes that “over 98% of stolen laptops are never recovered.” Also “notebook theft is the 2<sup>nd</sup> most prevalent computer crime, following virus related offenses” according to a CSI/FBI PC Crime and Security Survey.

When your laptop is stolen, you not only lose the hardware, you lose the data on the hard drive. This happened to my daughter, an architecture student at the University of New Mexico. She lost much of her portfolio of architecture projects in her first two years because of this theft. As with most laptop owners, some of the data was backed up and some was not. We replaced the laptop but the sense of violation and loss was still there. She still misses that Fujitsu P2046 laptop, as she really liked it.

Think what would happen to you business or home records if your laptop was stolen. Even if you have it backed up and replace the computer, you will probably feel violated by the theft. There is also a psychological cost that is often not thought of until it happens to you. You would have no idea of where or if your data on the laptop was stored on some criminal's computer waiting for the opportune time to steal your identity, or pull some other crime against you. You would not

know if one of the many laptop drives sold on web auction sites was the one out of your laptop, or even if that laptop “just like yours” being auctioned was in fact yours.

As you can see, laptop security encompasses a number of things. Many of these things are not really very difficult or even very technical. They do take some thought, planning and often some research to find out the best way to counter some of the threats that are out there today.

The good part is that there are many security resources which can be very helpful and useful available on the internet today. Many software and hardware suppliers, like Microsoft, and Dell for example, have extensive security information, articles, whitepapers and books available. Many county, state and federal agencies, such as the [Department of Homeland security](#), [FBI](#) and [CERT](#), also have extensive security suggestions and information available for protecting your laptop, desktop computer, and computer network.

For Your Safety

H. Court Young

Promoting awareness through the written word

<http://www.hcourtyoung.com>

<http://www.tmcco.com>

©July 2004