

## Risk Management Disciplines – Desktop & Mobile Systems (ISO § 4.2)

### Setting up Your Computer

The following tips are presented in an order that should help prevent a new or restored computer from being compromised by an attacker or worm on a hostile network, while you are in the process of setting it up.

- 1) **Services** - disable unnecessary services (developing...)
- 2) **Configuration** - review security configuration parameters and modify as necessary (developing...)
- 3) **Firewall** - use a **personal firewall** to protect your system when connected to a network.
- 4) **Updates** - maintain your system with current software versions and updates to improve functionality and reduce vulnerability to attacks.

**Windows Update** - Microsoft Windows systems

- 5) **Anti-virus** - Use **virus protection** software in case you inadvertently introduce an infected file into your computer or stray to a hostile web site.

### Using Your Computer

Setting up your computer as advised above is a good start; however the following practices are also advised to protect your computer and sensitive information on a daily basis.

- 1) **Web Browsing** – How to protect yourself from malicious web page links: **Microsoft knowledge base article (833786)**
- 2) **Email** - when handling email, practice more secure **email disciplines**.
- 3) **Identity Theft** – Learn more about identity theft, how to protect yourself, and how to report incidents: **Identity Theft Defense**
- 4) **File Sharing** – All forms of file sharing, even diskettes or CDs, involves risk unless precautions are taken.
  - **File Sharing, Including Peer-to-Peer**
  - **Copyright Violations**
- 5) **Downloads** – downloading free software is not recommended because of the potential for spyware or malicious code. While there are numerous responsible and reputable sites that provide free software, sorting them out can take considerable time. Note that “popular” does not necessarily mean “reputable”. Add a layer of **spyware protection** if you download free software.
- 6) **New Technologies** – new technology can be compelling, but often introduces risks that are not well understood until later.
  - **Camera Phones**

---

## **Benefits**

Adopting security disciplines like those described above will:

- help protect your information
- help to prevent your system from being hijacked and used by attackers against others on the Internet.
- increase pressure on less considerate companies to engineer stronger products and services
- increase effort and reduce benefits for attackers, reducing more "recreational" or beginner hacking, and make it easier to catch more advanced hacking techniques as security staffs will be less busy responding to mischief

Avoiding security disciplines will lead to **increasing legislation** and:

- increased government involvement along with related costs
- in some cases unnecessary restrictions for businesses and individuals, with increased effort and costs
- in some cases less privacy from government involvement
- lawsuits from information exposure
- loss of confidence in the Internet

## **Resources**

**Security Wisdom** 

**Trustworthy Computing: Security** - Microsoft site with update information and security guidance

**Security at Home** - Lots of info about Service Pack 2, Protect Your PC, Top Security Tips, spyware, phishing, etc.

**Apple Product Security** - Apple website with update information and security guidance

**CERT Home Computer Security** - Great information source to protect your PC. - Courtesy of CERT

**Home User's Security Checklist for Windows** - SecurityFocus.com

Securing Windows XP step-by-step (available shortly)