



# Managing Your Windows PC

## Skills for the Electronic Workplace

Stephen Carr, IST-Client Services, University of Waterloo

December 10, 2004

Copyright © 2004, IST SEW

Permission to use this document for non-commercial purposes, in original or modified form, is granted, provided that the original source of the document is acknowledged as Skills for the Electronic Workplace, Information Systems and Technology, University of Waterloo, Canada.

---

## Table of Contents

Managing Your Windows PC.....	1
What is Computer Management and Why Should I Do It?.....	1
Defining the Perils.....	2
How is Windows Vulnerable?.....	3
Security Management Strategy.....	4
Setting Up A New PC With XP Home.....	4
What About XP Professional Or Other Operating Systems?.....	5
Firewalling Network Services.....	5
Windows Update Service and UW's Software Update Service.....	6
Limiting User Account Privileges.....	6
Data Privacy.....	7
Protecting Against Malware.....	7
Passwords.....	9
Physical Security.....	9
Data Security.....	9
Maintaining System Performance.....	10
Reference Links.....	10

### ***What is Computer Management and Why Should I Do It?***

You might think that managing your computer is something optional, something done to fix some bugs or add the latest features to your operating system and applications. If things are working OK, it is easy to overlook or put off management tasks. Today, however, taking action against attacks that arrive over the Internet is the primary reason for managing your computer. Unfortunately, some of these attacks pose real threats to your privacy and could expose you to theft of your money, or your identity. Even worse, out of the box, your Windows PC is not in the most secure configuration. Management is no longer an option.

PC management comprises several activities:

- updating and patching your operating system and applications
- account management: creating user accounts and assigning privileges to those accounts
- securing your network connection(s) with a firewall
- monitoring for and removing viruses, worms and Trojan horse programs
- monitoring for and removing spyware and adware
- physically securing your PC
- protecting your data with backups
- maintaining system performance

In this course we will focus on how to manage a computer running Windows XP Home Edition. However, some mention will also be made of the older Windows 95/98/ME and the more feature-laden Windows XP Professional, and, briefly, alternative operating systems.

## ***Defining the Perils***

Let's be clear about what the threats are. Malevolent software, or “**malware**”, is commonly classified into several categories that describe the basic mechanisms by which it is spread (but in reality there is a lot of overlap among them):

### **Viruses**

These are programs designed to “infect” your system. They replicate, like a human virus, when run. You must deliberately run them for them to do any damage. They often arrive as email attachments. They generally need to be run by a privileged user (an administrator) to do any serious damage. Another form of virus is the **macro virus**, designed to infect Microsoft Office, through the Visual Basic macro language used to automate Office applications. Opening a macro-virus-infected document with macros enabled can cause subsequent documents that you created to be infected. The virus is spread when you send an infected document to someone else.

### **Worms**

These programs can self-propagate and replicate over the Internet, exploiting security holes in applications or system software. Often, no user interaction is required for them to do damage and to spread. They can be particularly malevolent. For example, a worm could install a “back door” on your computer to allow remote access and control, or a keyboard logger to capture account names and passwords. Many worms are called “**bot worms**” because they turn your computer into a robot or “**zombie**” that performs automated tasks for the attacker.

### **Trojan Horses**

These are programs that masquerade as something they are not. You must deliberately install and run them as a privileged user for them to do any damage. A Trojan horse could also install a back door, keystroke logger, or “bot” scripts (see Worms, above).

## **Spyware/ Adware**

Programs, usually bundled with other software, that collect personal information, or that pop up ads. These programs must also be deliberately (though usually unwittingly) installed by a privileged user. Peer-to-peer file sharing applications are notorious purveyors of spyware and adware. You may be agreeing to install spyware or adware when you accept a software license agreement, if you have not read it carefully. Spyware is perhaps the greater security threat of the two, because personal information is collected without your knowledge. Adware is at least designed to alert you of its existence. Both spyware and adware may also severely degrade the performance of your system.

## **Phishing**

Conning people to provide their private information, using email or the web. Phishing does not typically involve any tampering with your PC.

Regardless of how the malware gets to your computer, once run, it can help someone to perpetrate several kinds of attacks:

### **Hardwarehijacking**

Someone takes over your computer, remotely, without your knowledge. There are numerous ways to do this. The new “owner” of your computer can use it as a base to attack others, thus hiding his tracks. Your machine could also be set up as an automated “zombie”, attacking other computers over the network, perhaps causing a denial of service. Hardware hijacking may also be perpetrated by a local attacker, someone who has physical access to your computer.

### **Denial of Service**

A computer (yours or someone else's) slows to a crawl or stops working. Often this is accomplished against a commercial web server by swamping it with numerous simultaneous requests from thousands of zombies. Or a denial of service can be directed (intentionally or unintentionally) against your PC, by degrading its performance or destroying your data. Viruses, worms, spyware / adware, Trojans, and saturation of network services can all cause this.

### **HardwareFailure**

A final threat to your system that usually has nothing to do with malware is hardware failure. If your hard disk fails you may lose personal data that you've spent a lot of time accumulating. Rarely, there are bugs in hardware device drivers that may be exploited by an attacker to damage the hardware.

## ***How is Windows Vulnerable?***

Is Windows any more vulnerable to malware than any other operating system? Yes. Windows has been more of a target for attack than other operating systems. Much of the software is designed to attack vulnerabilities in the Windows XP operating system. Also, other operating systems cannot run software that is compiled to run under Windows, so most viruses, Trojans, spyware, etc., are ineffective. Finally,

a common characteristic of the types of malware outlined above is that they must be installed by a privileged user. Windows, by default, makes every user an administrator with complete control over the computer, even though accounts with lesser privileges are available. Programs run by an administrator run with the privileges of an administrator. This allows malware free reign to do its damage. Other operating systems usually provide user accounts with lesser privileges by default.

## ***Security Management Strategy***

### **1. Fortify**

- Minimize network services (have fewer doors)
- Firewall (guard the doors)
- Update and patch (keep up with maintenance)
- Strong passwords (lock the safe)
- Few administrators (few sets of keys to the safe)
- Physical security, BIOS password, restrict boot options (prevent insurrections)

### **2. Trust Nobody**

- Monitor and clean viruses, worms, Trojan horses
- Don't fall for scams ("phishing" expeditions)
- You get what you pay for: search for and remove adware / spyware
- Read all agreement forms. Beware if they are hundreds of pages long.

### **3. Carry Insurance**

- Keep backups of your data
- Keep an image of your working operating system

## ***Setting Up A New PC With XP Home***

If installing from CD,

1. Install initially without a network connection (wired or wireless)
2. Do "Custom Settings" for the network setup, then uncheck "Client for Microsoft Networks", "Quality of Service (QoS)" and "File and Printer Sharing" on all network connections.
3. Enter the product key

The computer will reboot... then (this will be the state of a pre-installed system)

1. Ensure Internet Connection Firewall (or Windows Firewall, for Service Pack 2) is enabled on all network connections, in Network Connections control panel.
2. Plug in to the network, and configure your Internet connection according to the instructions from

your Internet Service Provider. Then enable Windows Update Service in the System control Panel (under Performance and Maintenance).

3. Apply any updates.
4. Downgrade privileges of your own user account to “limited” and make unprivileged accounts for your family members.
5. Set passwords on all accounts and make them “private” if you are worried about privacy of data. **N.B.** If an account profile is made private, not even administrator can see what’s in it!
6. Set a password on the Guest account by Start / Run: “net user guest <the-password>”. The Guest account is used for all network connections.
7. Set a password on the hidden Administrator account by Start/ Run: “net user administrator <the-password>”. The administrator account is only usable in Safe Mode (entered by pressing the F7 key when booting).

### ***What About XP Professional Or Other Operating Systems?***

XP Professional has more security features, but also more networking features. It can be made more secure than XP Home, but requires more knowledge (and tweaking) to do so. It also exposes more network services to attack. Unless you want to connect your PC to a Windows network (join a Windows domain) you probably don't need Windows XP Professional. Besides support for networking and centralized management, there are only a few important features provided by Windows XP Pro that are unavailable in XP Home [1]:

- remote desktop access to your PC from another location
- more fine-grained control over shared files
- encrypted file system support for secure data storage
- support for multi-lingual user interface

### ***Should You Upgrade From Windows 95/98/ME?***

Yes, if your hardware is capable of running XP. Even if your computer can run XP, older versions of Windows have a performance advantage over XP on older hardware. However, XP is superior with respect to stability (propensity to “crash”).

Older versions of Windows were not designed for security. Specifically, any user of the system has administrator powers, and there is no effective way to protect the system with a password, or protect different users' files on the same computer. This is bad for controlling infections by malware. You will also be open to local tampering (do you trust your kids?). The main disadvantage of running an older version of the OS is that new software will not likely be supported. However, as long as you have software that works for your needs, you might be tempted to maintain the status quo. Indeed, having an old OS may prevent some malware from running, that is, software that was designed to attack XP. Windows 95/98/ME has the further properties that it does not expose network services, and is a less popular target for attacks than Windows XP. However, there is still a large amount of malware that can infect Windows 95/98/ME.

If XP is not possible and you want to keep using your PC, you still need to be careful that your OS is updated to the latest patch level, is running antivirus software and a firewall. Also make sure that you are not running any old software that has well documented security exploits, for example, an old versions of Outlook or Internet Explorer.

If you are wondering about alternative operating systems, MacOS and Linux are well designed OSs that can be made very secure. While they still need to be managed with respect to security patches, they are definitely less popular targets for attacks at present (and not vulnerable to Windows exploits). In fact Linux runs very well on older hardware, so it might be a more secure option for keeping alive that old workhorse.

## ***Firewalling Network Services***

Network services are programs that run in the background and enable various kinds of communication over the network. Each (TCP) service uses one or more “ports” for its communications. A port is a software construct rather than a physical device; it's an address for a service. For example, Web traffic is directed through port 80. Your computer can be attacked through any running network service if there is a bug associated with it. The best defense against such attacks is not to run any network services that you don't need. Windows XP Home has fewer network services available than Windows XP Pro since it is not designed for a corporate environment (which usually has a large number of networked and centrally managed workstations).

There are numerous network services that you want or need to have running, for example the Windows update service. A firewall is a network service used to protect other services from worms and direct attacks. A firewall is software that controls network traffic. The simplest type of firewall controls traffic at the port level, e.g., blocking all incoming traffic that is not responding to a request initiated by your PC, except for traffic on ports that you specify. This prevents “probing” attacks. The built-in firewall in Windows XP works in this way. There are more sophisticated firewalls that can block both incoming and outgoing traffic, and can control traffic more finely, e.g., according to which computers it comes from. These more sophisticated firewalls are provided by third-party vendors such as Norton [2], McAfee [3], and others. ZoneAlarm, by Zone Labs [4] has a free product for non-commercial use.

As a minimum, Windows XP's built-in firewall should be enabled on all network connections. With Windows XP Service Pack 1 (SP1), the firewall is called Internet Connection Firewall; it is not enabled by default. To do so open the Network Connections control panel, right-click your network connection and get Properties. Select the Advanced tab and check Protect My Computer. If you have updated to SP2, the firewall is called Windows Firewall and it is activated by default. If you have a laptop and will be wanting to connect to UW's wireless network [5], you must adjust your firewall(s) to allow ICMP remote echo request (a.k.a “ping”) through (follow the previous link for instructions).

## ***Windows Update Service and UW's Software Update Service***

Windows Update Service is the built-in updating tool for Windows XP. It provides OS and MS application updates over the network, through a web interface, directly from Microsoft. Windows Update is useful for home users. If you don't have a fast Internet connection, UW Home & Security CD has recent updates to pre-install (avoiding large downloads). It's also safer to update your PC as much as possible before you connect to the Internet.

At UW, IST offers a Software Update Service (SUS), which is a local mirror of the Microsoft updates (operating system updates only). The advantage of using UW's SUS service are:

- Faster downloads
- Pre-tested updates (it's been known to happen that updates can cause problems of their own).

The UW SUS service [6] is intended mainly for on-campus PCs, but can be used from off campus as well.

## **Updating your Applications**

It's a good idea to keep your application software updated as well, particularly network clients such as web browsers and email readers. Non-Microsoft browsers and email clients are often safer to use because they aren't tightly bound to the operating system, and are not as frequently attacked. You'll need to remember to visit the vendor's web site directly to get any bug fixes or security updates.

## ***Limiting User Account Privileges***

Windows XP provides the ability to create separate accounts for each user of your PC. It is a good idea to do this. However there are some specific steps you need to take to do it correctly. By default, Windows XP Home gives all user accounts administrator privileges, and does not set a password. This is a bad thing if you want to control the spread of malware, as outlined above. Lack of strong passwords, particularly on administrator accounts, lets anyone with access to your PC install or modify anything. Also, without passwords you can't have any privacy (more on this in the next section).

Windows XP Home allows you to reduce the privileges of accounts to **limited** status. Limited accounts can run (most) installed software but cannot modify the operating system or (usually) install their own software. It is a good idea to designate one or two administrators for your PC to set it up and install software. But for daily use of the PC, everyone should use their own limited account. This ensures that any OS modifications or additions of software are intentional. Make sure all administrator accounts have a strong (not easily guessable) password. Don't forget to set a password on the built-in, but hidden, account called "administrator" (see **Setting Up A New PC with XP Home** above).

This account strategy may not work well if you want to run older programs and many games, since these will often fail to run with the privileges of a limited account. For such software that is still being developed and sold, it would be a good idea to contact the vendor to request that they modify the software so that it can run as a limited user. There is also a work-around for this problem. Create a separate account called, e.g., "games", give it administrator privileges and a password that is shared with those who need to run the software. Then when someone using their limited account needs to run a game, they do so with the "**runas**" feature to run it with administrator privileges. Runas can be run from a command shell (Start/All Programs/Accessories/Command Prompt, then run the command "runas /help" for instructions). You can also find the program you want to run with elevated privileges through My Computer or Start/All Programs/Accessories/Windows Explorer, then right-click on it and select Run As. **Note**, however, that having fewer "administrators" means less chance of installing malware. Always start people off with limited privileges and only increase them if absolutely necessary.

## ***Data Privacy***

With Windows 95/98/ME there is no privacy of users' files. Windows XP Home allows separate accounts for each user and provides the opportunity for privacy of data files. However, by default Windows XP Home allows any user to view the files of other users. User accounts can be made private by an administrator. To do so locate the user's local folder (called the local **profile**) at C:\Documents and Settings\userid, right-click the folder, then select Sharing and Security and Make This Folder Private. **Note** that any user accounts that are made private in this way become inaccessible by others thereafter, even an administrator.

For another layer of security, XP Professional (but not Home) has Encrypted File System support, which allows users to encode any files they want to make unreadable by anyone else.

Another measure to ensure the privacy of your users is to use password-protected screen savers (set in the System control panel under the Display tab). Also take measures to detect and remove spyware (see the next section).

A final topic to be aware of is "phishing". Phishing describes the act of conning people into giving away their user Ids and passwords or other valuable information such as SIN numbers, credit card numbers, etc. Phishing is often done through email, faked to look like it comes from Microsoft or your bank. It usually tells the recipient to go to a web site (again faked to look official) and provide the desired information, or download an operating system "patch" that is a Trojan horse. You should be aware that no legitimate company would use email to ask you to do these things. If you still are not sure, call the company to check out the suspicious request before you do anything. Phishing is the method by which most serious crimes such as identity theft are perpetrated.

## ***Protecting Against Malware***

Having limited user accounts is the most effective way to protect against having people inadvertently installing viruses, Trojan horses and the like. There are also software tools that help detect and remove malware when it arrives at your PC.

### **Antivirus Tools**

Log in and run applications as an unprivileged user if at all possible. Virus detection software is also a must in a multi-faceted security scheme. The UW Home and Security CD [7] has a site-licensed copy of Symantec Antivirus. It can also be downloaded from [www.ist.uwaterloo.ca/download](http://www.ist.uwaterloo.ca/download). Symantec Antivirus may be configured to get automatic updates of its virus definitions from Symantec, or from UW [8]. Running an antivirus tool helps protect you from known problems, but does not protect you from new viruses. Some antivirus tools will warn you about any program that is acting like a virus, thus giving you some measure of protection in that regard.

Defense against macro viruses involves disabling macros and write-protecting your macro definitions file. Microsoft Office has built-in defenses against the spread of macro viruses now, so they are less of a problem than in the past. Also, using a different office suite (e.g., the free OpenOffice [9] suite, or StarOffice [10] which is free for educational use at UW) can protect you, while allowing you to maintain compatibility with Microsoft Office document formats.

## **DefenseAgainstInternetWorms**

Worms are often spread by exploiting open (not password-protected) network shares or other network services with known bugs. Worms can also be propagated via email (sending worm-laden email from you to those listed in your address book). An effective way to avoid that is to use an email reader other than Outlook or Outlook Express, since these are often the targeted transmission mechanism. Mozilla Thunderbird and Eudora are free alternatives to the Microsoft email clients. Instant messaging has also become a common way for worms to travel, through its file sharing mechanism, similar to an email attachment. Turning off file and printer sharing on all connection types in the Network Connections control panel is recommended (See Setting Up A New PC With Windows XP Home, above). Keeping your operating system up to date with the latest updates is essential in order to repair known problems that could be exploited by a worm. A third-party firewall that controls outgoing as well as incoming network traffic can prevent a “bot worm” from sending data to an attacker, or from attacking other computers. Antivirus tools can identify and remove many known worm infections, if the virus definitions are kept up to date.

## **DefenseAgainstTrojanHorses**

Log in to your computer and run all applications as an unprivileged user if at all possible. There is little automated protection available against Trojan horses, except for those being delivered through email or via Internet worms that may be detected by your antivirus software. In particular, be wary of peer-to-peer file sharing. The quality of executables obtained that way is suspect, particularly pirated commercial software. The maxim “you get what you pay for” applies here. Download programs only from trusted sites (and verify that they have not been tampered with by using “check sums”, if available).

Trojan horses often make use of the fact that, by default, Windows hides the extensions on the names of known file types. This viewing property allows Trojans to be easily disguised, for example, a file called **photo.jpg.exe** will show in Windows Explorer as **photo.jpg**. It is a good idea to disable this viewing property on all folders for each user of your PC. This is done through My Computer/Tools/Folder Options/View. Uncheck the option “hide extensions of known file types” and click the “Apply to All Folders” button.

## **DefenseAgainstSpyware/Adware**

Log in and run applications as an unprivileged user if at all possible. Avoid peer-to-peer file sharing. Just installing a peer-to-peer client may install spyware and adware (read the license agreement, but you may not even be told). Run Spybot [11] and/or Ad-Aware [12]. Both are free-for-noncommercial-use downloads. You'll need to keep these updated to have the latest detection capabilities.

## **Passwords**

Passwords are required to protect the privileges of administrator accounts and protect the privacy of regular users' data. All remote access to Windows XP Home from the network is done through the built-in **guest** account, so make sure it has a password too—it doesn't by default (see Setting Up A New PC with XP Home, above). Use strong passwords:

- No dictionary words or names. If you want to use a word or name in your password, put other characters or numbers between some of its letters.
- Use at least three different character types: capital letters, lower case letters, numbers, non-alphabetic characters.
- Choose passwords that you can remember without having to write them down. If you do write them down, don't write the user ID and password down together.
- Use a different password for each account you have. You can probably think of a clever way to remember which password is for which account.

Protect your passwords, particularly those for UW accounts that you access remotely. Only use encrypted protocols to log in to remote computers (SSH and SCP/SFTP instead of telnet and FTP). Make sure you use encrypted protocols when logging in over the web too, e.g., HTTPS (Secure Socket Layer encrypted) log-in to [www.mywaterloo.ca](http://www.mywaterloo.ca) [13] to read mail and get files.

Any unfamiliar computer should not be trusted. Keystroke loggers that run on the computer are a common way to obtain account names and passwords. Beware of logging in to any accounts from Internet cafés. Change your passwords frequently if you must use untrusted computers to access your accounts.

### ***Physical Security***

Anyone with access to your PC and sufficient time can take it over (your kids wouldn't do that, would they?). Prevent people from booting from other than the local hard disk by adjusting the BIOS boot settings (pressing Delete or some other key during a reboot gets you into the BIOS). Set a BIOS password so that settings can't be changed without it. Locking the computer case is the only way to prevent the BIOS password from being reset, but perhaps that is not practical or necessary for home PCs.

### ***Data Security***

Backups are your last defense against loss of your data. But they are easy to ignore ... until it's too late. Writeable CDs and DVDs are a good, cheap option for backups. Protecting your personal data [14] is first priority. Save your work often and get into the habit of backing up your work every day that you make a change. Really important data should be stored in a fireproof box away from your computer.

XP Home (also Windows ME) has a built-in System Restore feature, enabled in the Performance and Maintenance control panel under System. It is run by booting into Safe Mode (press the F7 key during a reboot), then looking under Performance and Maintenance in the Start menu. There are also commercial applications to back up your entire hard disk to CDs (e.g. SyQuest Drive Image).

### ***Maintaining System Performance***

The last aspect of computer maintenance that we will consider is system performance. The basic rule is that if you want your system to perform better, add more RAM. If you are using Windows XP, you should have at least 256 MB of RAM, more if you can afford it.

A data file is not necessarily stored in one piece on your hard disk, but is broken up to fit into the

available free space. Eventually your system will slow down because it has to reconstruct every file you open from many pieces. Defragmenting the hard disk puts the files back in order and consolidates the free space on the disk. It's a good idea to defragment your hard disk regularly, perhaps monthly. The Defragmenter is located in Start/All Programs/Accessories/System Tools.

Windows runs many local and network services. These use system resources (memory and CPU cycles). It is possible, though not necessarily recommended, to disable non-essential services that you are not using. There are sites on the web [15] that list services that you can safely disable. It is not a good idea to disable security-related services, such as Windows Firewall.

### ***ReferenceLinks***

1. XP Home vs. XP Professional: [www.microsoft.com/windowsxp/pro/howtobuy/choosing2.msp](http://www.microsoft.com/windowsxp/pro/howtobuy/choosing2.msp)
2. Norton Personal Firewall: <http://www.symantec.com/>
3. McAfee: <http://www.mcaffee.com>
4. Zone Labs: <http://www.zonelabs.com/>
5. UW's wireless service: <http://www.laptop.uwaterloo.ca/>
6. UW's SUS service: <http://www.istiis.uwaterloo.ca/sus/>
7. UW Home and Security CD: <http://ist.uwaterloo.ca/cs/homecd.htm>
8. UW Symantec Antivirus Update Service: <http://ist.uwaterloo.ca/ps/services/antivirus.html>
9. OpenOffice: <http://www.openoffice.org/>
10. StarOffice: <http://www.sun.com/software/star/staroffice/>
11. Spybot: [www.safer-networking.org/](http://www.safer-networking.org/)
12. Ad-Aware: [www.lavasoftusa.com/software/adaware/](http://www.lavasoftusa.com/software/adaware/)
13. UW's MyWaterloo secure web email: <http://www.mywaterloo.ca/>
14. Ten ways to protect your personal data: <http://www.ist.uwaterloo.ca/cs/safecomp.html>
15. Bob Cerelli's Windows tips site: [http://www.onecomputerguy.com/windowsxp\\_tips.htm](http://www.onecomputerguy.com/windowsxp_tips.htm)
16. UW IST's Security How-Tos: <http://ist.uwaterloo.ca/security/howto/>