HOME PC SECURITY IN WINDOWS XP

Home PC Security

Andrew Miles
Microsoft Australia
7 February 2006

Transcript of presentation delivered to the
PC Users Group
7 February 2006
By Andrew Miles, Microsoft Canberra

Table of Contents

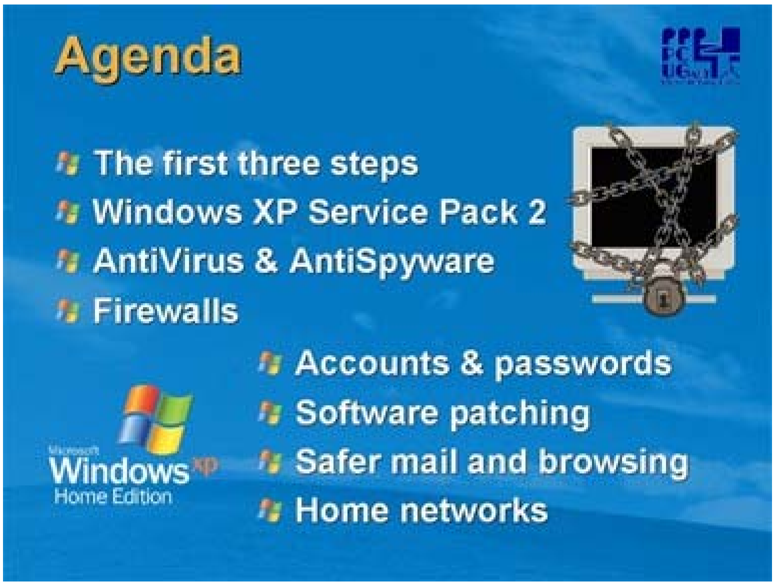
The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

This deliverable is provided AS IS without warranty of any kind and MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OR OTHERWISE.

Introduction

Today's presentation will cover aspects of protecting your Home PC from common threats. It is targeted at an "end-user" audience – those of you with an IT background will be familiar with the concepts but hopefully there's something for you also. The content is targeted towards Windows XP SP2 Home Edition but the concepts are relevant to all Home PCs, especially different flavours of Windows. There are some additional features in XP Pro that you may well be familiar with but we'll focus the discussion on what most users will have on their home PC. Our basic message is to protect your PC and personal data as you would your credit cards and important documents



Agenda

- The first three steps
- Windows XP Service Pack 2
- AntiVirus & AntiSpyware
- Firewalls
- Accounts & passwords
- Software patching
- Safer mail and browsing
- Home networks

Microsoft
Windows xp
Home Edition

You don't need to lock your PC away and be paranoid about security. Basic housekeeping and common sense will keep you protected. We'll cover the essentials of a protection strategy, starting with the First Three Steps – firewall, automatic updates and antivirus – and the tools Microsoft has incorporated into Windows to make these easier for you.

If you don't already have Service Pack 2 we strongly recommend it. We'll talk about some of the technologies in it that will help you stay secure.
Then a little on some of the tools available to you – often for no cost – to protect your system; antispyware, antivirus and firewalls. What they are and why you should have them.

Windows 2000 and Windows XP use the concept of individual users on a machine to keep your personal data private. We'll discuss how this works specifically in an XP Home environment and how we recommend you set your system up.

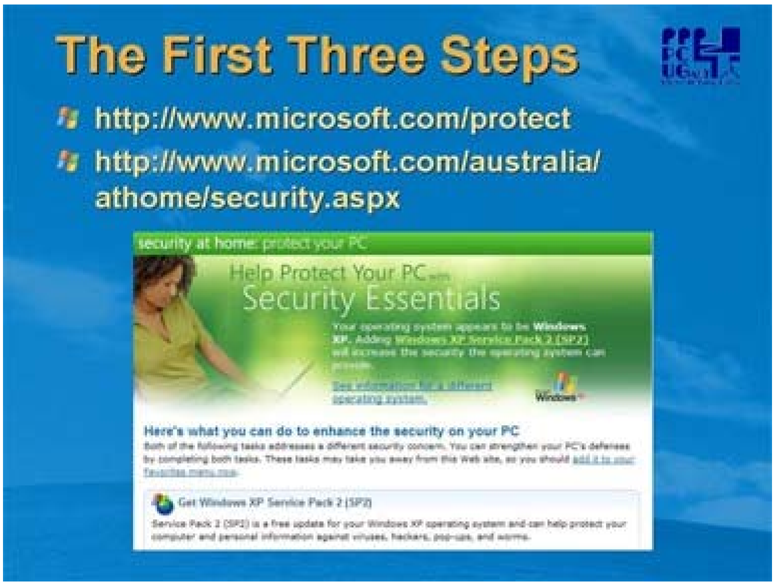
Keeping your system (not just the operating system itself) current is important and we'll cover the basics of that.

Most malicious software (commonly now called "malware") is imported onto your system through email attachments and malicious web sites. We'll share with you some simple ways you can minimise the risk of infection through these sources. We'll talk a little about identity theft too and this "phishing" you may have heard about.

Finally we know many homes now have networks installed. These can be a real boon to those with a number of PCs and a need to "roam" around the house, and the good news is these can really help with your security environment if they are configured and managed correctly. We'll show you how.

In essence, you wouldn't leave your home unprotected and unlocked, and it isn't a major imposition for you to secure it before you go away. Properly managed, securing your PC will similarly become second nature to you.

The First Three Steps



The First Three Steps

- http://www.microsoft.com/protect
- http://www.microsoft.com/australia/athome/security.aspx

security at home: protect your PC

Help Protect Your PC with Security Essentials

Your operating system appears to be **Windows XP**. Adding Windows XP Service Pack 2 (SP2) will increase the security the operating system can provide.

See information for a different operating system.

Here's what you can do to enhance the security on your PC

Both of the following tasks addresses a different security concern. You can strengthen your PC's defenses by completing both tasks. These tasks may take you away from this Web site, so you should add it to your Favorites menu now.

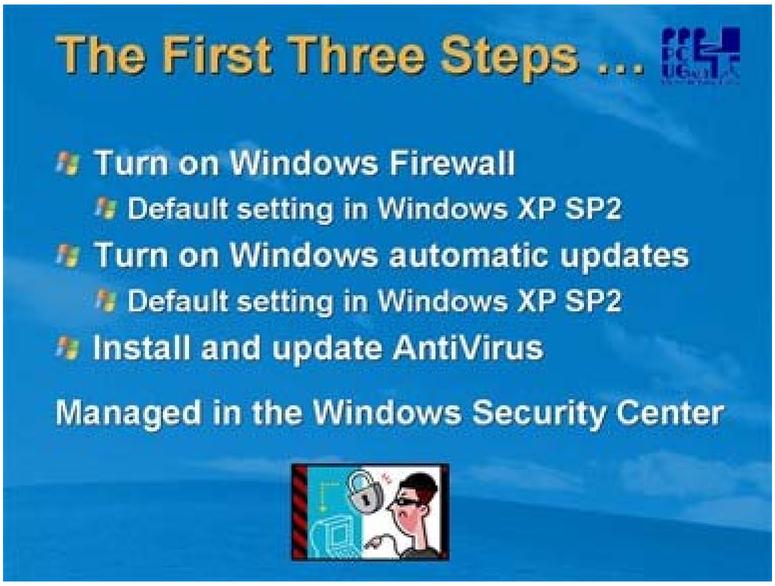
Get Windows XP Service Pack 2 (SP2)

Service Pack 2 (SP2) is a free update for your Windows XP operating system and can help protect your computer and personal information against viruses, hackers, pop-ups, and worms.

The first three steps - if you do nothing else to your PC, ever, simply taking these three steps will give you a significant head start. I've noted here a couple of useful web sites where these are documented in detail, so please take the time to review these after the session.

The screen shot is from the first of these websites. It will take you through the steps, even allowing you to take the suggested actions whilst online. The first two of these involve enabling features already installed in Windows, whilst the third requires a third-party solution to be installed. You may find that your PC already has this – most major manufacturers include an anti-virus solution in their package at time of purchase.

You can use this site regardless of what version of Windows you are running, but you'll have most protection if you're running Windows XP SP2. If you have SP2 installed already, the screen you see will look slightly different in that it will recognise you have SP2 and present different options.



The First Three Steps …

- Turn on Windows Firewall
  - Default setting in Windows XP SP2
- Turn on Windows automatic updates
  - Default setting in Windows XP SP2
- Install and update AntiVirus

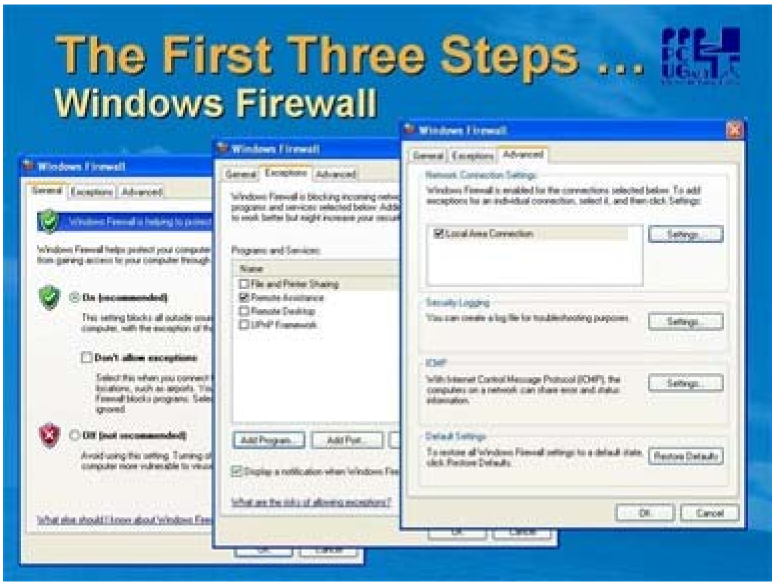
Managed in the Windows Security Center

Don’t worry about remembering all of this, we’ll be covering each of these in more detail shortly. In summary:

- Turn on the Windows XP firewall (or install a firewall if running an earlier version)
- Turn on automatic updates (setting will depend on your network connectivity)
- Install and update an AntiVirus solution INCLUDING an automatic update capability (virus signature files are updated very regularly to deal with new threats)

All sounds too hard? Don’t worry - Windows XP SP 2 added the new Security Center feature to help you manage all of this easily from one interface. We’ll have a look at that in a while.

These together will maximise your chances of keeping out the evil dude at the bottom.



The First Three Steps …

Windows Firewall

Windows Firewall

General | Exceptions | Advanced

○ On (recommended)

□ Don't allow exceptions

○ Off (not recommended)

Programs and Services:

□ File and Printer Sharing
☑ Remote Assistance
□ Remote Desktop
□ UPnP Framework

☑ Display a notification when Windows Fi…

Network Connection Settings

Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:

☑ Local Area Connection

Security Logging

You can create a log file for troubleshooting purposes.

ICMP

With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.

Default Settings

To restore all Windows Firewall settings to a default state, click Restore Defaults.

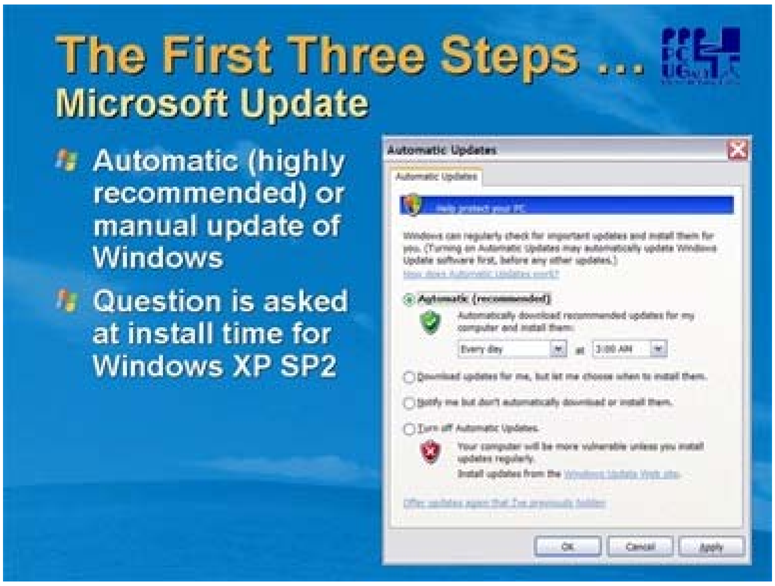
We’ll talk a little later about what a firewall is, but for now lets just have a look at the interface for the Windows Firewall. It’s available via the Control Panel (if you’re not sure where that is, hit the Start Button and it’s one of the options halfway down the second column. If you click on this you’ll get all the Control Panel options. Click on the icon called Windows Firewall).

The first screen more or less begs you to leave the firewall on. If you have a native Windows XP SP2 installation it will be on by default. If you have upgraded it may not be on, depending on your original configuration before you upgraded. The “Don’t Allow Exceptions” option is designed for mobile users, who may have a laptop they use to access many networks. It allows them to turn of the exceptions when connected to a “less trustworthy” network.

You can set up your exceptions on the “Exceptions” tab. Exceptions are programs that are allowed through the firewall. Some of these may actually be set by the installers themselves, and some will require manual setting. If you don’t set an exception, you’ll get a message to say a communication was blocked, and you’ll be asked if you want to add it to the exception list. “File and Printer Sharing” is a common exception and must be checked if you have a home network (more on this later).

The “Advanced” page won’t be used by most users – the key point here is that there are many firewall settings that can be changed on a “per connection” basis – that is, traffic types that are allowed on one connection (for example whilst connected to a home network) and not on another (for example a wireless hotspot).

More on firewalls later.



The First Three Steps …

Microsoft Update

- Automatic (highly recommended) or manual update of Windows
- Question is asked at install time for Windows XP SP2

Automatic Updates

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

● Automatic (recommended)

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Microsoft Update is an automated update tool for Windows environments. It's been around since Windows Me days but in Windows XP it is a more prominent part of the UI. You may be familiar with the original Windows Update version which has now been replaced by the wider-reaching Microsoft Update functionality.   Microsoft Update is essentially a superset of Windows Update and includes other Microsoft software in its scanning – at this stage Office XP and 2003, Exchange 2003 and SQL 2000 are included.

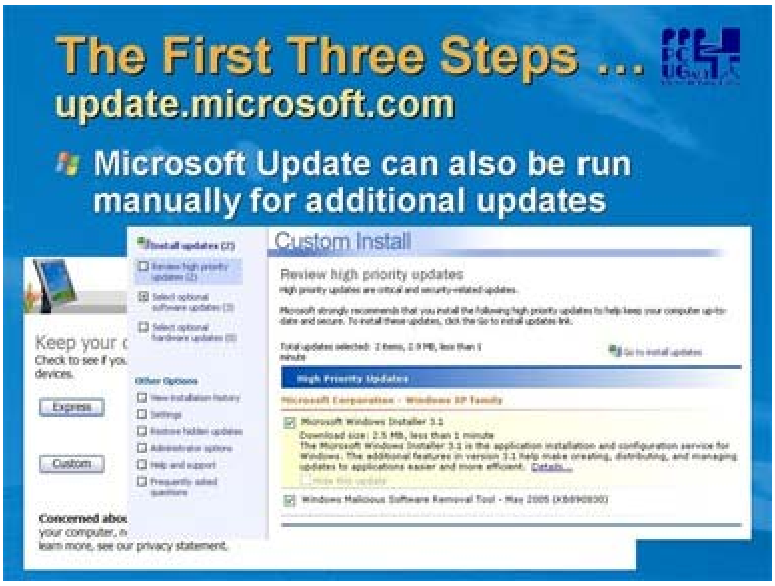
Microsoft recommends you set your system up for Automatic Updates (from the "Automatic Updates" icon in Control Panel).

Update options recommended depend on your setup.

- If your PC is on and network connected constantly, select Automatic and a time every night
- If you have a broadband connection but are not permanently networked, select "Download and choose"
- If you have intermittent or dial-up networking, select "Notify"

Please do not select "turn off" unless your PC is completely standalone

Will happen in the background – no user intervention required. May require a reboot, so be aware of this if you are allowing the system to install these overnight.



The First Three Steps …
update.microsoft.com

- Microsoft Update can also be run manually for additional updates

Install updates (2)
□ Review high priority updates (2)
☒ Select optional software updates (3)
□ Select optional hardware updates (0)

Other Options
□ View installation history
□ Settings
□ Restore hidden updates
□ Administrator options
□ Help and support
□ Frequently asked questions

Custom Install

Review high priority updates
High priority updates are critical and security-related updates.

Microsoft strongly recommends that you install the following high priority updates to help keep your computer up-to-date and secure. To install these updates, click the Go to install updates link.

Total updates selected: 2 items, 2.9 MB, less than 1 minute

Go to install updates

High Priority Updates

Microsoft Corporation - Windows XP Family

☑ Microsoft Windows Installer 3.1
Download size: 2.5 MB, less than 1 minute
The Microsoft Windows Installer 3.1 is the application installation and configuration service for Windows. The additional features in version 3.1 help make creating, distributing, and managing updates to applications easier and more efficient. Details...
□ Hide this update

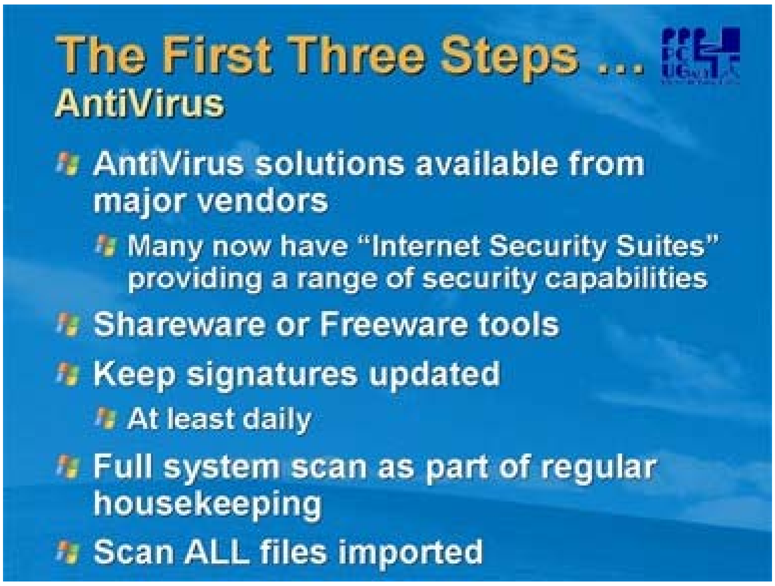
☑ Windows Malicious Software Removal Tool - May 2005 (KB890830)

These screen shots are from the update.microsoft.com website and are what you will see if you go to Microsoft Update manually (Start | All Programs | Microsoft Update).

This interface allows you to install other non-critical components and updates (for example, Windows Media Player 10 is delivered this way). Hardware drivers are also made available through this channel. A word of caution – you may find that some updates have prerequisites, and you need to run manual Microsoft Update more than once to ensure you have all patches. Microsoft suggests you leave the setting on Automatic unless your network connection is intermittent.

As with automatic updates, you may have to reboot. You are given the option to do this immediately or later, to give you the opportunity to close any open work.

As a guide I recently rebuilt a Windows XP SP2 system and connected to Windows Update directly after installing SP2 and was offered around 17MB of updates – a significant reduction from XP base and SP1 systems.



The First Three Steps …
AntiVirus

- AntiVirus solutions available from major vendors
  - Many now have "Internet Security Suites" providing a range of security capabilities
- Shareware or Freeware tools
- Keep signatures updated
  - At least daily
- Full system scan as part of regular housekeeping
- Scan ALL files imported

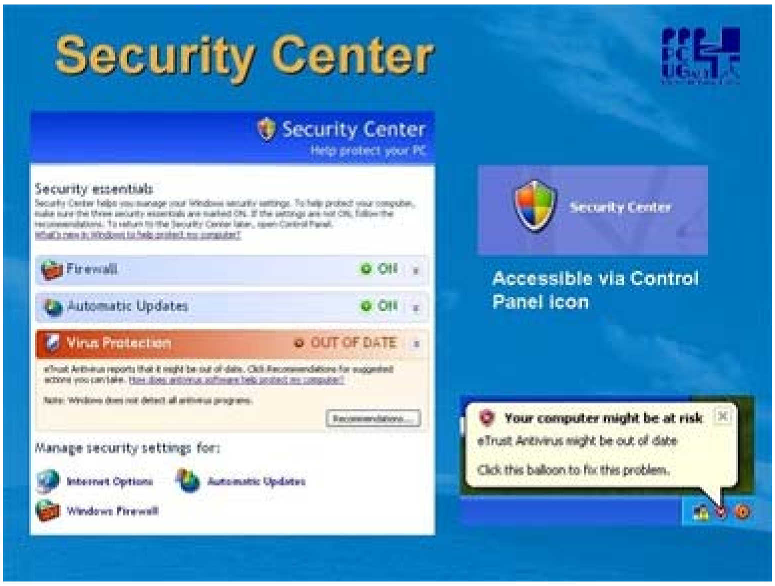
Viruses are unwanted programs that find their way onto your computer through various means. Once installed, they can cause a number of problems from sluggish performance through to data loss and system compromise. They commonly then use your machine to launch attacks on others, often through your contact list.

The best way to prevent the actions of a virus is to ensure they can't get a foothold in your system, which means using an Anti-Virus tool. All PC systems should have anti-virus protection. There are many reputable offerings in the market place, from full-function security suites to freeware. Microsoft does not currently offer an AV solution, but may do so in the future.

Most "branded" PCs sold today include an anti-virus product and/or subscription. These are definitely worth taking up.

Key to effective anti-viral activity though is good housekeeping – scan ALL files imported into your PC (there have even been isolated incidences of viruses on packaged product CDs), keep signature files updated at least daily and do regular system scans. The most sophisticated tools available won't help if you allow programs to execute without safeguards.

If your product has an automatic updating facility then set this up. If it requires a manual signature download, schedule this as part of your daily routine.



Security Center

Security Center
Help protect your PC

Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall ● ON
Automatic Updates ● ON
Virus Protection ● OUT OF DATE

eTrust Antivirus reports that it might be out of date. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Manage security settings for:

Accessible via Control Panel icon

Your computer might be at risk
eTrust Antivirus might be out of date
Click this balloon to fix this problem.

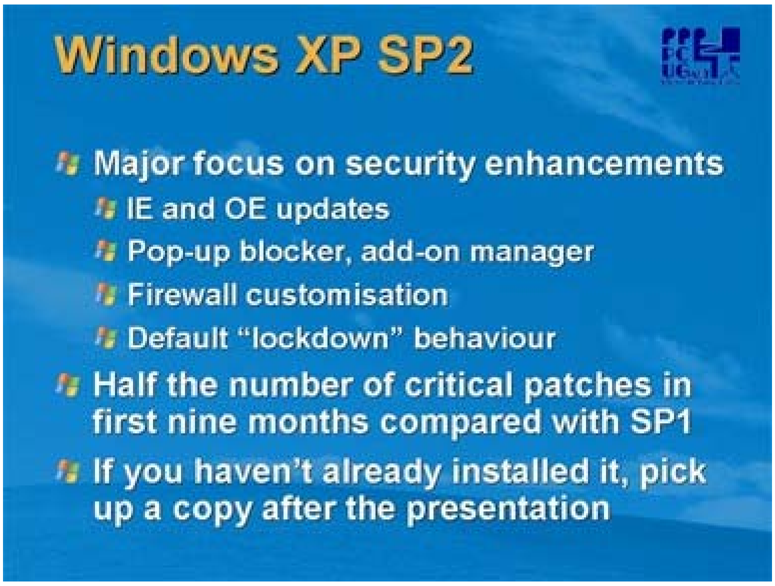
This applies to Windows XP SP2 only.

To assist you in ensuring that the protection available from firewall, automatic updates and anti-virus is effective, SP2 includes the Security Center – a new icon on the Control Panel, and the first place you should check for any security-related concerns on your PC.

Further, Security Center itself will alert you if there are any settings in these three areas which deviate from "best practice" and make suggestions as to how to fix them. An example is shown here, where the eTrust Antivirus product on this system has not been updated recently and may be an exposure.

A Red Security Center icon in your system tray denotes a security exposure that you should correct as soon as possible.

Why Windows XP SP2?



Windows XP SP2

- Major focus on security enhancements
  - IE and OE updates
  - Pop-up blocker, add-on manager
  - Firewall customisation
  - Default “lockdown” behaviour
- Half the number of critical patches in first nine months compared with SP1
- If you haven’t already installed it, pick up a copy after the presentation

Just one slide on Windows XP SP2. It was released in August 2004 and some 300 million copies have been installed, so it’s a fair bet that if you have a Windows XP system you have already done the upgrade. If not, please either download it from Microsoft update or order yourself a copy from Microsoft.

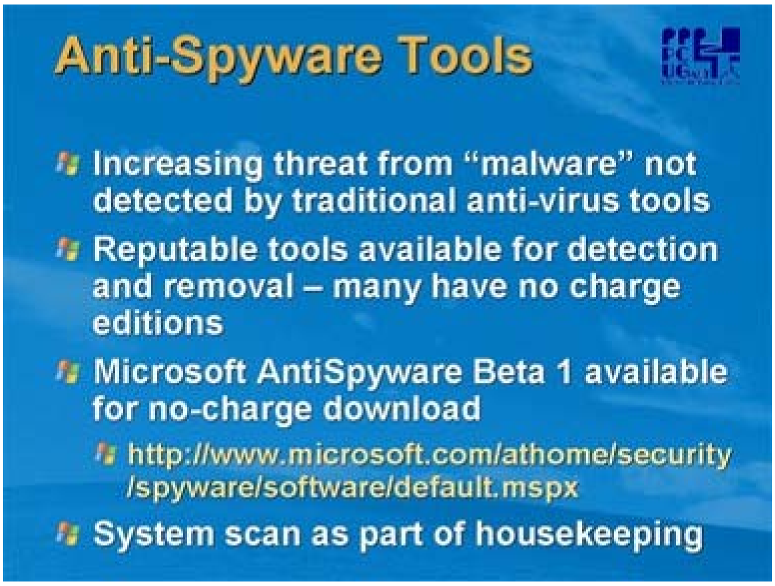
Microsoft made security a key commitment in SP2. We worked hard to ensure that there were tools to make sure the system was more secure by default and provided as much defence as possible against malware. We’ll focus here on a few of the features improving security for home users

- Security Center, mentioned above
- IE pop-up blocker
- IE add-on manager
- IE scripting and code management improvements
- Changes to IE and OE default settings and improved granularity
- Firewall improved customisation
- Firewall and many security settings on by default

We’ll cover some of these in more detail later.

SP2 has had a significantly lower patch rate than either Windows XP or SP1 did in the first nine months of release, so it requires significantly less effort to keep your system current. Microsoft now also has a monthly patch release cycle, so you can better plan your patch download activity.

Anti-Spyware Tools



Anti-Spyware Tools

- Increasing threat from "malware" not detected by traditional anti-virus tools
- Reputable tools available for detection and removal – many have no charge editions
- Microsoft AntiSpyware Beta 1 available for no-charge download
  - http://www.microsoft.com/athome/security /spyware/software/default.mspx
- System scan as part of housekeeping

The traditional viruses and worms are being supplanted by a new class of electronic pest called "spyware". Spyware is a generic term for code that finds its way onto your system and is used to surreptitiously record usage information (for example, track your web site history or keyboard key strokes) and transmit this information to a third party.

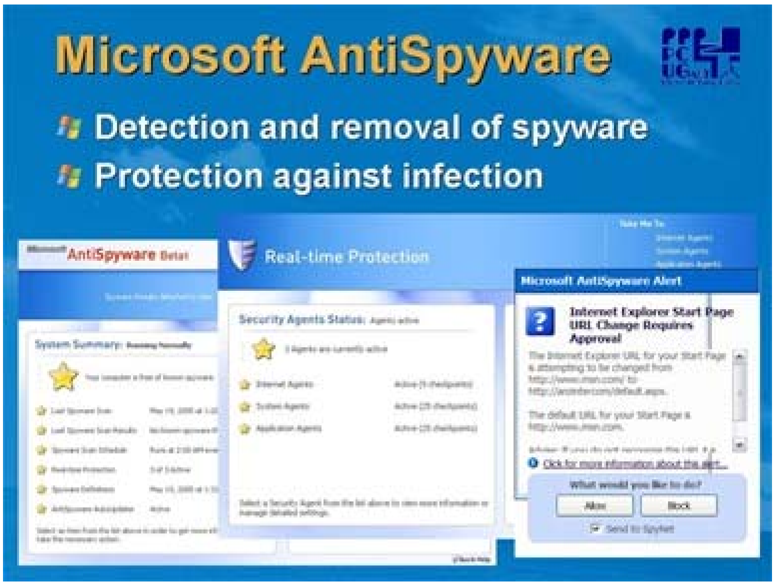
Some spyware is "legitimate" – your Cookies folder for example stores information about various web sites you have visited, and you may wish that information to be kept so the next time you go back to a particular site, your history is recalled. However, as a general rule, any piece of such code that you did not explicitly install yourself should be considered malicious.

Spyware is often promulgated through malicious websites that use tools like pop-ups – hence the measures taken in SP2 mentioned previously.

Microsoft recommends that you install and maintain an anti-spyware tool. You may find your anti-virus suite includes such a tool and you can integrate the management of both. Microsoft has a tool in this space currently in a beta release and available for free public download at the above site.

As with anti-virus tools, ensure there is regular signature file updates and you perform system scans as part of regular maintenance. You should find your tool can set up both of these to run automatically, so it shouldn't be a major overhead.

As an aside, current plans are that the Microsoft AntiSpyware product will become part of Microsoft Defender and we have committed that a version of the technology will remain available free of charge to home users.



Microsoft AntiSpyware

- Detection and removal of spyware
- Protection against infection

AntiSpyware Beta
System Summary:
Real-time Protection
Security Agents Status:
Internet Agents
System Agents
Application Agents
Microsoft AntiSpyware Alert
Internet Explorer Start Page URL Change Requires Approval
Click for more information about this alert...
What would you like to do?
Allow
Block
Send to SpyNet

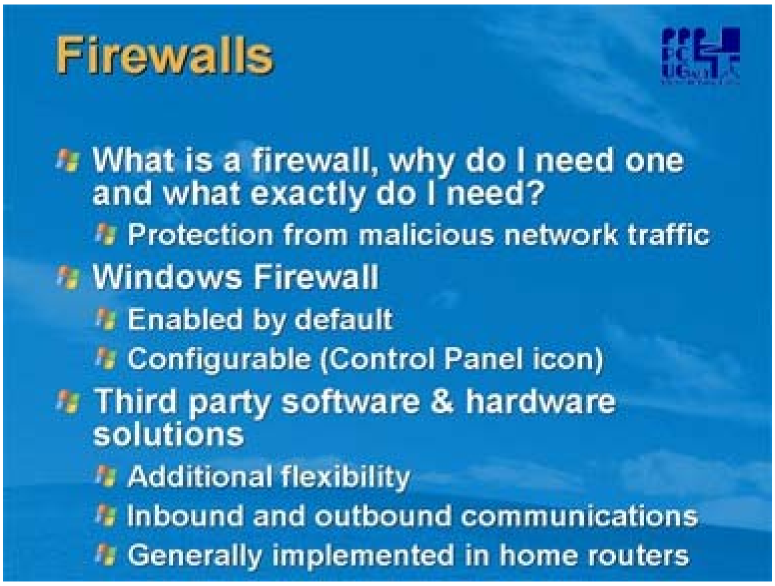
A couple of screen shots from the Microsoft AntiSpyware beta product. This product combines the ability to schedule updates and scans as well as manage a number of agents that monitor changes to key system variables and settings. Should one of those be changed by a user or a software program, you will be notified and asked whether the change is to be approved – much like a firewall will do with information requests to and from the network.

MAS can be used to clean the machine’s history to avoid it being made available to third parties – not just IE sites but recently opened documents, file locations and the like. It can be set to run in “knowledgeable” or “novice” user modes so the user is not inundated with messages and settings they don’t understand.

Intelligent updating through the SpyNet service where suspected spyware activity can be reported (with user approval) to a global community for analysis and if necessary anti-spyware definition updates. Also shown here is an example of a MAS message that pops up when MAS detects something that is wanting to change or update a setting that has been protected. In this case the user is being asked to approve the change – in the event of some occurrences (eg known spyware trying to run) blocking will be automatic if the agents are active.

Microsoft has stated that current plans are for a production version of this tool to be available in the home user marketplace free of charge. There may also be enterprise versions for businesses and/or subscription services for premium content.

Firewalls



Firewalls

- What is a firewall, why do I need one and what exactly do I need?
  - Protection from malicious network traffic
- Windows Firewall
  - Enabled by default
  - Configurable (Control Panel icon)
- Third party software & hardware solutions
  - Additional flexibility
  - Inbound and outbound communications
  - Generally implemented in home routers

A firewall is any solution (hardware or software) which monitors communication streams to and from a system, typically from an external network (in our case, the internet). It can also filter this communication, reject certain types of network traffic and "hide" the configuration of your network from the outside world.

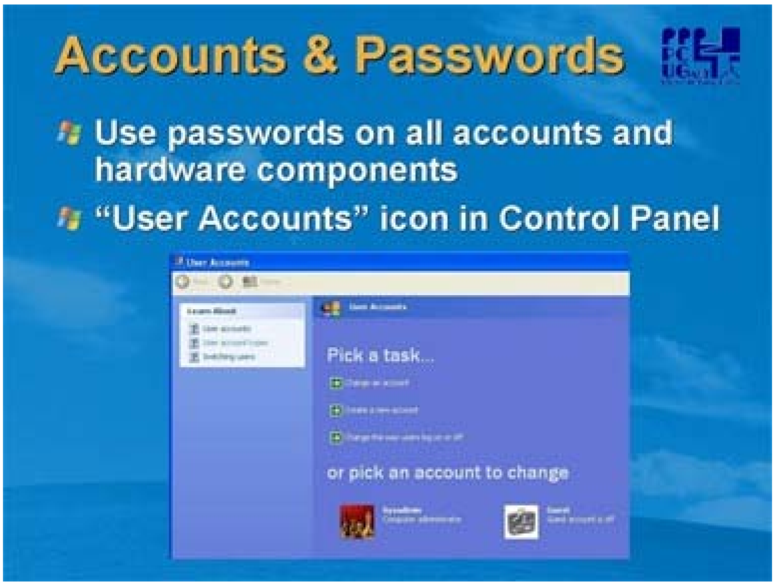
We've already spoken a little about Windows Firewall. This is a software firewall that monitors inbound network traffic and rejects that which is not specifically requested by programs on your "exception" list – remember these are programs you have explicitly authorised to communicate with others across the network (MSN Messenger is a simple example). Windows Firewall is a sufficient solution for most users, but some way wish a firewall that does "two-way" communication.

In this case there are third-party software options (fee and free) and again some of the "security suite" vendors include firewall technology. You do need to be somewhat careful though, as running a multi-layered firewall can cause problems. Windows XP SP2 is smart enough to recognise some third-party software firewalls (eg Zone Alarm) and turn off its own if an alternative is enabled.
Third party firewalls also potentially offer greater flexibility, but that also comes with the added overhead of having to manage another configuration.

The best solution for implementing a firewall for a home computer (whether or not you have a network at home) is a hardware device called a "router" (rhymes with outer). A router takes signals from one of the devices attached to it (be it local or a network connection) and figures out where they are supposed to go, and sends them on their way. A useful extra function of most routers is that they have hardware firewalls built in and provide advanced protection for any device attached to it. A router can also effectively "hide" the devices on your network from hackers on the internet. We'll cover home networking and routers a little later on.

So, in essence, if you're happy with Windows Firewall, leave it switched on. If you need additional protection, install and configure a third party solution and for real peace of mind, hide your system behind a hardware router. If you have or are considering broadband, consider installing an "all in one" modem, router and firewall device.

Accounts and Passwords



Accounts & Passwords

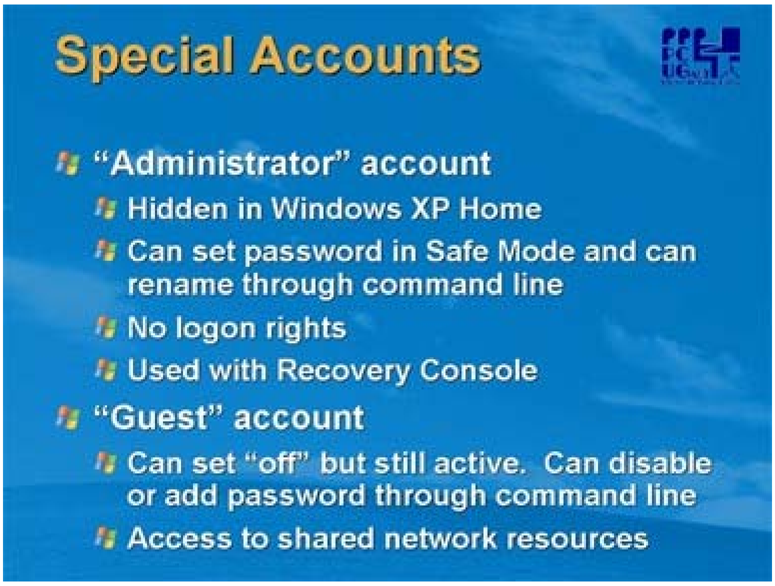
- Use passwords on all accounts and hardware components
- "User Accounts" icon in Control Panel

Windows 2000 and Windows XP have the ability to "fence" individual users on a computer. When you install Windows XP Home you will be asked for a user name and this username (sysadmin in the example here) becomes an administrative user on the system. However (and unlike XP Professional for any of you who have experience installing that) you do not have the option to provide a password. Microsoft recommends that you add a password to all users on a system, and to do this you use the "User Accounts" function from the Control Panel

You should password protect access to your system (including hardware devices and file shares) as a general policy, just as you use a PIN on your banking cards and a password for your email account. It just provides another level of security making it harder for someone to gain access to what is yours.
In the example here, you click on the "sysadmin" user and select "Change Password" from the next dialogue box that appears. The cost of this to you is that you need to explicitly logon with the password (there is a command line "tweak" to override this) when you start the computer, but you get extra security as a result.

You should also set passwords on any other hardware devices like routers in your network.

Lets talk about Windows XP accounts in a little more detail



Special Accounts

- "Administrator" account
  - Hidden in Windows XP Home
  - Can set password in Safe Mode and can rename through command line
  - No logon rights
  - Used with Recovery Console
- "Guest" account
  - Can set "off" but still active. Can disable or add password through command line
  - Access to shared network resources

A word of warning first up. These accounts work differently in XP Home to XP Professional. There are references in the Microsoft Knowledgebase at support.microsoft.com if you want to investigate this further.

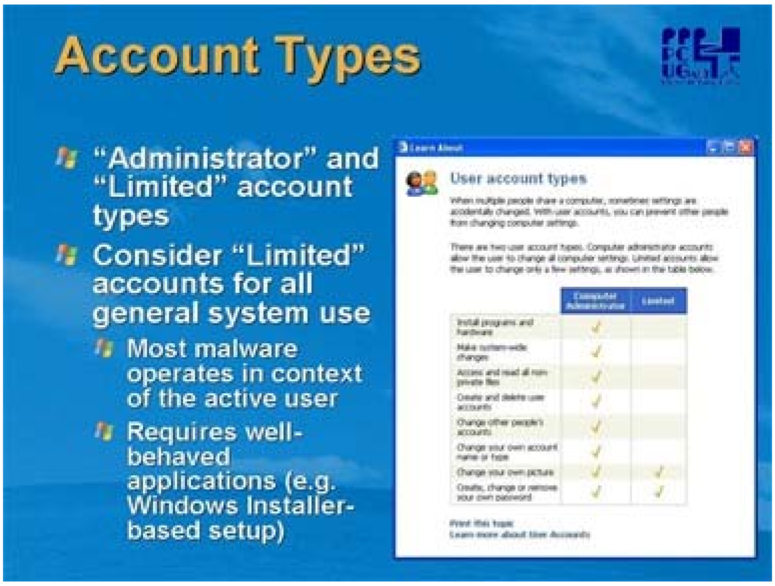
The Administrator account in XP Home is created automatically and cannot be disabled. It only appears visible in Safe Mode. It does not have a password assigned by default. Whilst this might seem like a security exposure, it is in fact there for a logical reason, and not a risk to your system. In XP Home, Administrator is prevented from logging on either locally or across the network onto the system unless the system is running in Safe Mode. If you specifically start the system in Safe Mode, then networking is disabled by default.

It is there simply as a recovery tool – if you forget the password of all other users, you can start the system in Safe Mode, log on as Administrator, and reset all other passwords. It also allows you to use the Recovery Console feature of Windows XP if you are unable to boot the system for some reason.

Our recommendation? If you are concerned about there being no password, start the system in Safe Mode and use Users and Groups to assign a password AND make sure you record this somewhere.

The other system account is the "Guest" account. Windows XP Home Edition will not allow you to disable the Guest account (unlike XP Professional). When you disable the Guest account in Windows XP Home Edition via the Control Panel, it only removes the listing of the Guest account from the Fast User Switching Welcome screen, and the Log-On Local right. The network credentials will remain intact and guest users will still be able to connect to shared resources of the affected machine across a network. Microsoft Knowledge Base Article 300489 describes this behaviour.

There is a command line option to assign a password to the Guest account or properly disable it if you wish but this has implications if you are using file or internet connection sharing. If you have only one PC on your network, go right ahead. The Guest account has very few rights and this creates a very minimal exposure.



Account Types

- "Administrator" and "Limited" account types
- Consider "Limited" accounts for all general system use
  - Most malware operates in context of the active user
  - Requires well-behaved applications (e.g. Windows Installer-based setup)

User account types

When multiple people share a computer, sometimes settings are accidentally changed. With user accounts, you can prevent other people from changing computer settings.

There are two user account types. Computer administrator accounts allow the user to change all computer settings. Limited accounts allow the user to change only a few settings, as shown in the table below.

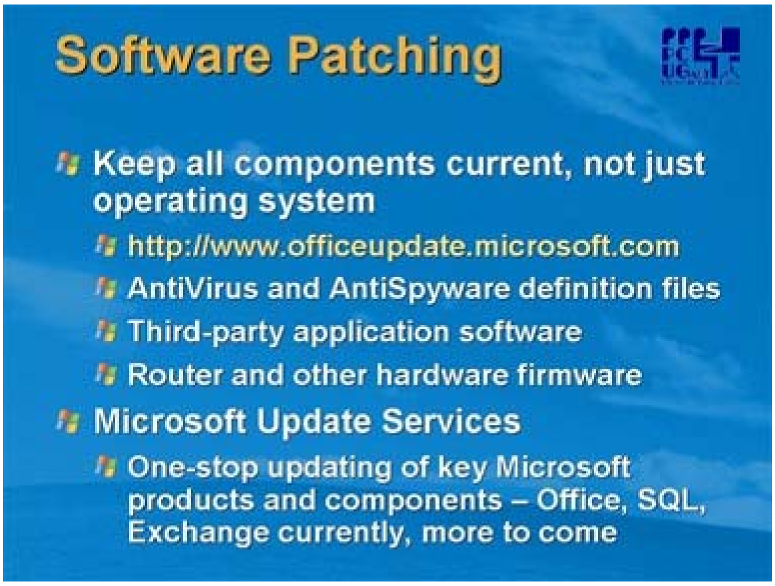
	Computer Administrator	Limited
Install programs and hardware	✓	
Make system-wide changes	✓	
Access and read all non-private files	✓	
Create and delete user accounts	✓	
Change other people's accounts	✓	
Change your own account name or type	✓	
Change your own picture	✓	✓
Create, change or remove your own password	✓	✓

Now, let's assume you have built your system and created your initial Administrative account. What now? Windows XP allows you to create additional users with different capabilities – in the case of XP Home these are either "administrator" or "limited" users. The rights of each user class are shown here. So why is this useful? As most malware has to be physically installed on your system, and also operates in the context of the user running it, it makes a great deal of sense to set up users on your system as "Limited". That way, firstly the chances of inadvertently running malicious code is reduced and secondly even if it is run it can't do as much damage (eg can't update the registry).
If you set up an account for each user of the system as Limited, and leave the Administrator account for system management activity, you significantly reduce the attack surface. You also create a "private" environment for each user.

A disclaimer here is that you may find some of your software doesn't run in a limited account – typically anything that is Windows Installer compliant will be OK (as it is installed in an administrative context regardless of the user) but some games and older software may have problems. There are some "tweaks" to get around this, such as not using the "Program Files" folder for the installs, using the "Run as" command or running applications in compatibility mode.

But certainly use Limited accounts, for example, for children browsing the net and/or running email applications. I have a separate administrator account for running ill-behaved software and have disabled other capabilities of this account. Yes, any administrator who knows what they're doing can reverse this, but it's better than nothing.

Software Patching



Software Patching

- Keep all components current, not just operating system
  - http://www.officeupdate.microsoft.com
  - AntiVirus and AntiSpyware definition files
  - Third-party application software
  - Router and other hardware firmware
- Microsoft Update Services
  - One-stop updating of key Microsoft products and components – Office, SQL, Exchange currently, more to come

OK, so we run Microsoft Update and get all the patches we need for everything? Well, unfortunately it isn't quite that simple (yet) and you do need to be diligent about updating your software environment. All software needs patching from time to time and most major manufacturers either have an updating service or will at least provide update patches.

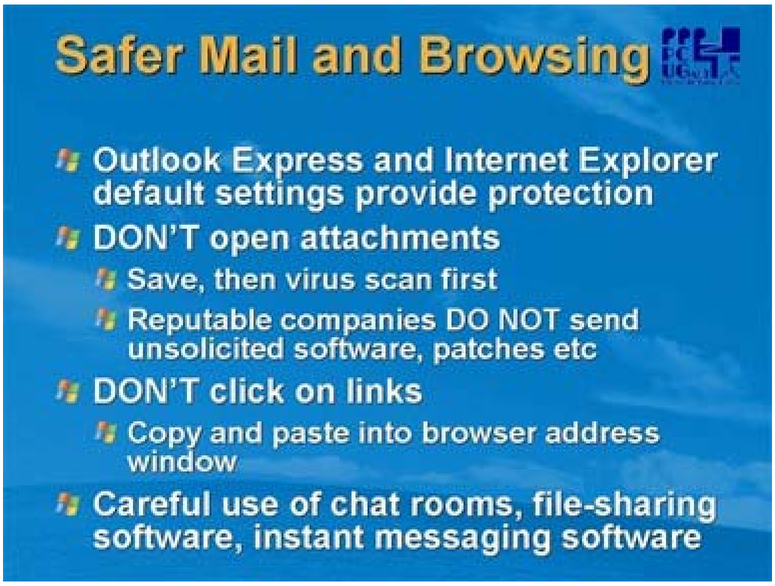
If you have Microsoft Office or any Office product you can also update via the officeupdate site as shown. This works like Microsoft Update in that it detects your Office environment and provides only the patches you need.

You must keep antivirus and antispyware tools updated, preferably using the "live updaters" that usually come with such tools. If you don't wish to do this or there are no facility to do this, make sure you download signature files regularly.

All the non-Microsoft software on your system should be maintained also. Many major applications now test for this automatically (eg Adobe Acrobat) but it is worth keeping a note of manufacturers web sites and subscribing to any patch bulletin services offered. Also your router or other hardware access device will have firmware which may be periodically updated by the vendor to provide additional security or patch known bugs.

Microsoft Update Services combines the original Windows Update with an update capability for other Microsoft software, including Office, Exchange and SQL Server. This will assist in at least keeping your Microsoft software current.

Safer Mail and Browsing



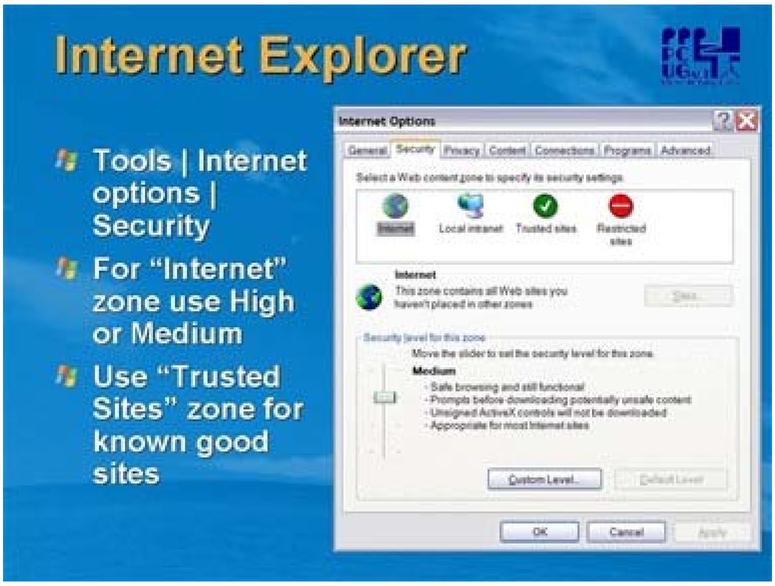
Safer Mail and Browsing

- Outlook Express and Internet Explorer default settings provide protection
- DON'T open attachments
  - Save, then virus scan first
  - Reputable companies DO NOT send unsolicited software, patches etc
- DON'T click on links
  - Copy and paste into browser address window
- Careful use of chat rooms, file-sharing software, instant messaging software

There are definitely steps you can take as an internet and mail user to minimise the threat to your system or network from malware. Internet Explorer (IE) and Outlook Express (OE) themselves provide a range of protection options, which are generally "on" by default in Windows XP SP2. So here are some very basic rules.

- NEVER open attachments in an email. In OE, as we'll see in a couple of slides, attachments are blocked by default, but if you have enabled them make sure you always save then virus scan anything you get sent. As an extra precaution in Windows XP SP2 you will be asked before you run any program that's been downloaded from a network. Reputable organisations DO NOT send patches as attachments – they instead provide notification of a patch and details as to how you can obtain it.
- DON'T click on links in email. Instead, either use the "Plain Text" option for mail display to ensure the link is as it claims to be, or simply "cut and paste" into your browser. That way the real address behind the link is revealed. We'll see an example of this shortly
- ANY software that allows your machine to be networked with others, but especially file-sharing programs, should be treated with caution. These programs are notorious for either being supplied with, or allowing through "backdoors", spyware code.

As a general rule don't allow anyone access to anything on your system, and if you must use peer-to-peer networking tools, use a separate PC that you do not keep sensitive data on.



Internet Explorer

- Tools | Internet options | Security
- For "Internet" zone use High or Medium
- Use "Trusted Sites" zone for known good sites

Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone
Move the slider to set the security level for this zone.
Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

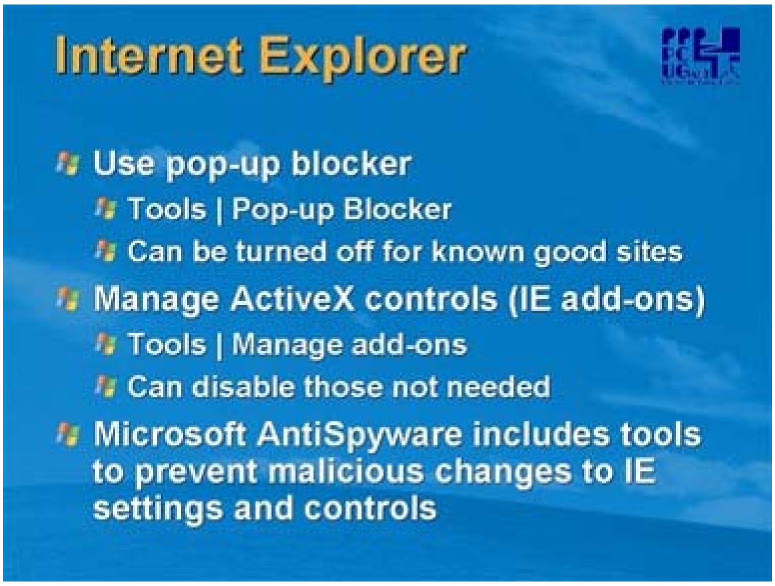
We're not going to go into too much detail with the settings but I just wanted you to know they were there and that you could "tweak" them if necessary. You'll find Windows itself provides a tight level of control by default, so if you never play with these you are pretty well covered. In addition, tools like Microsoft AntiSpyware monitor any changes to these, so if malicious code tries to "hack" your browser interface, you'll know about it.

In Internet Explorer 6, the relevant settings are managed from the Tools | Internet Options | Security menu, which displays the interface shown here. "Medium" or "High" is recommended for general internet browsing, with sites that you explicitly trust (for example your internet banking site) listed in the "Trusted Sites". Trusted Sites run in a "low" security context as it is assumed the code on them is safe. This provides the highest level of functionality. "If you click "Restricted Sites" you'll see a list of sites that are suspected of being able to damage your system – these are only accessible with the security level set to "High".

Naturally the user can change any of the specific sites or the security levels, but we don't recommend you do so unless you know your actions are safe.

If you hit "Custom Level" on any of these settings you'll see the complete list of configurable options, so if you know you need a specific capability but no others, instead of just setting the slider to a lower level, just change the specific setting. This will probably only happen if a site you trust, for example, requires a particular configuration item to be set.

In general, you won't need to do anything here except add sites to your trusted list. But it's useful to know that it's here if you need it.



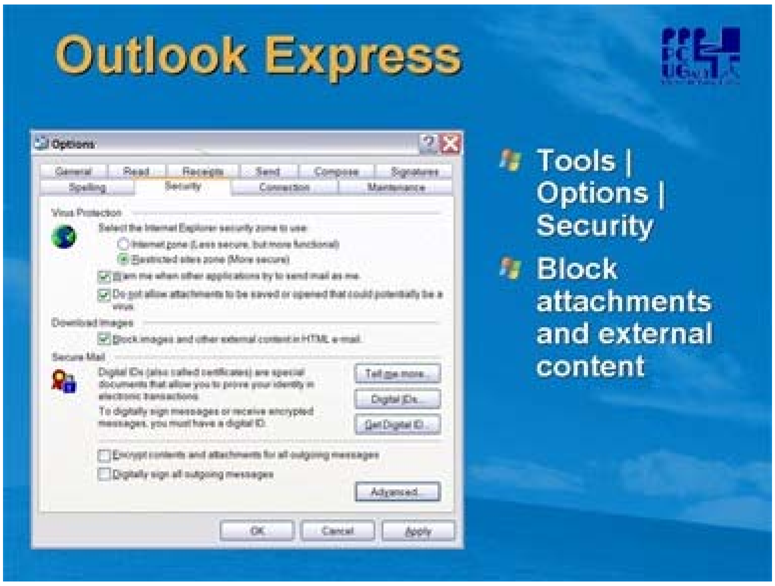
Internet Explorer

- Use pop-up blocker
  - Tools | Pop-up Blocker
  - Can be turned off for known good sites
- Manage ActiveX controls (IE add-ons)
  - Tools | Manage add-ons
  - Can disable those not needed
- Microsoft AntiSpyware includes tools to prevent malicious changes to IE settings and controls

One of the key features in Windows XP SP2 is the pop-up blocker. Pop-ups (either hidden or visible) are IE windows with new web sites that appear when you click what seems to be a different link. They are common sources of spyware, and particularly invidious when they don't actually appear to the user.
The Pop-up blocker is found as indicated, and can be set to High, Medium or Low. We recommend at least Medium, and setting an "exclusion" list of sites that you are happy to accept pop-ups from. Do not turn it off unless you have an alternative pop-up blocking mechanism.

When a site displays a pop-up and the blocker is on, you get a message in the IE information bar saying the pop-up has been blocked and giving you the option of unblocking it just for now or adding the site to the exceptions list. You can also set this to play a warning sound when this happens.
The other major new addition in IE is the add-on manager. Add-ons are modules written for IE by different software vendors to allow their programs to operate in a browser window. Common (and legitimate) examples are Adobe Acrobat Reader and Macromedia Flash. Now you can see and manage these programs in a single window, and disable any that do not appear to be valid or that you have not explicitly installed yourself.

As mentioned previously Microsoft AntiSpyware beta includes a number of IE Agents that notify you whenever a program attempts to change any of your default IE settings or, for example, tries to add a secure site.



Outlook Express

Virus Protection

Select the Internet Explorer security zone to use:

○ Internet zone (Less secure, but more functional)

● Restricted sites zone (More secure)

☑ Warn me when other applications try to send mail as me.

☑ Do not allow attachments to be saved or opened that could potentially be a virus.

Download Images

☑ Block images and other external content in HTML e-mail.

Secure Mail

Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.

To digitally sign messages or receive encrypted messages, you must have a digital ID.

□ Encrypt contents and attachments for all outgoing messages

□ Digitally sign all outgoing messages

- Tools | Options | Security
- Block attachments and external content

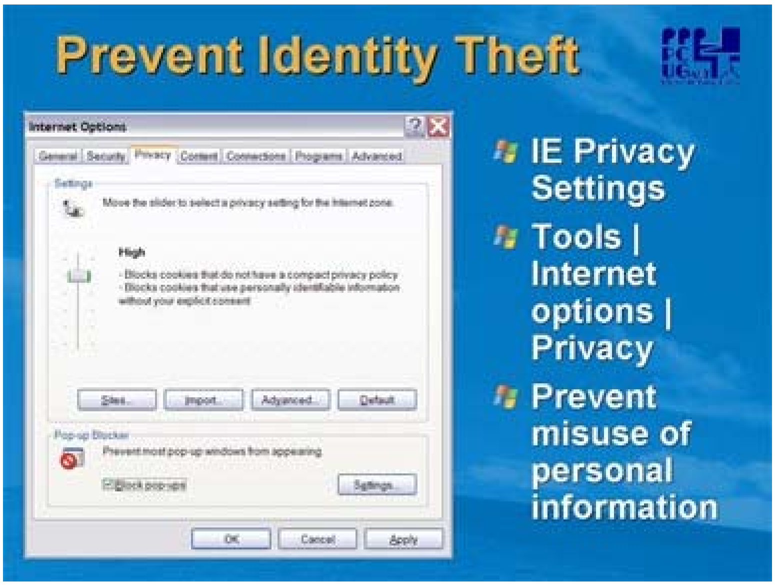
Turning now to OE there are some basic security settings here as well that can help you keep out unwanted software. The screen here is available from the OE Tools | Options menu and the Security tab. Firstly, Microsoft recommends you run OE in the context of the "Restricted Sites" zone (set by default to "High" security) to minimise the risk from active content in emails.

The "warn when other applications" option should be checked to prevent against the type of viruses that spread using your email contacts or address book. These are now less common as they are easier to stop in this way, but it's worth leaving this setting on anyway. When set on, any program that sends mail in your user context is intercepted and you have to explicitly allow it to proceed.

It's generally better also to check the "Do not allow attachments" option unless you are very careful with your attachments. If you check this, then any email with an executable attachment will be displayed with a message in the information bar saying that the attachment has been blocked. A hint here – if you really want that attachment that's just been blocked, go into this dialogue box, uncheck this option and go back to the email. You'll find the attachment is now available to you (but go and check the box again afterwards to remain protected). Attachments like word documents, emails and the like will remain visible to you.

"Block Images" is designed to remove active components from emails that may be suspicious. You'll see the impact of this when you see an email with pictures missing and a message to the effect that OE has blocked access. You'll be given the opportunity to download this content for this particular email if you trust it.

Protect Against Identity Theft



Prevent Identity Theft

Internet Options

Settings

Move the slider to select a privacy setting for the Internet zone.

High

- Blocks cookies that do not have a compact privacy policy
- Blocks cookies that use personally identifiable information without your explicit consent

Pop-up Blocker

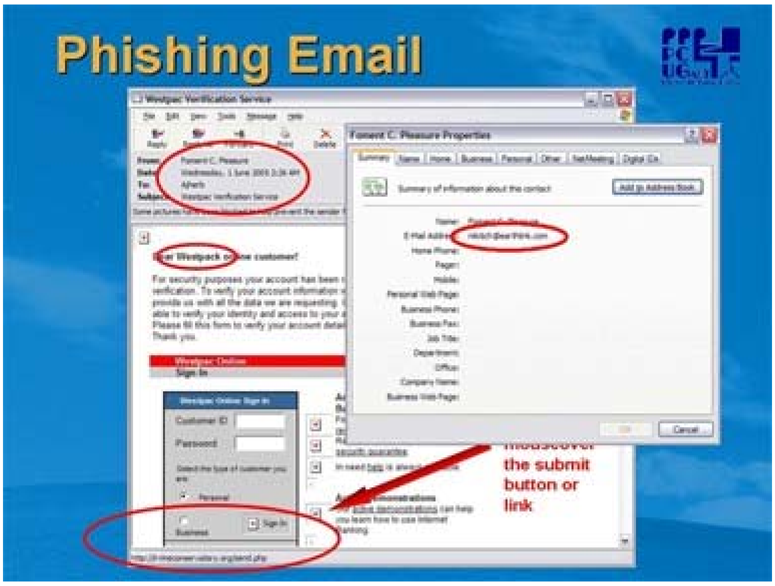
Prevent most pop-up windows from appearing

☑ Block pop-ups

- IE Privacy Settings
- Tools | Internet options | Privacy
- Prevent misuse of personal information

The issue of identity theft is gaining attention as software manufacturers work to provide better protection against the traditional threats to a computer system. Identity theft is a more insidious threat as the method of attack is often directed more at the user than at any particular flaw in the computer system. You can take some action to assist here in IE by managing the "Privacy" settings. You'll see here that the setting refers to what IE will do with "cookies". Cookies are small pieces of information kept on your computer that potential identify you, or particular aspects of your browsing or internet security history. Many of these are harmless, and might identify, for example, which page you last visited on a particular site, and you may wish that information to be stored. However, cookies are common targets for spyware, and should be protected as shown here. There is also a "Block all cookies" setting which provides maximum protection, but may impact your browsing experience.

However, the real protection against identity theft is vigilance – many attempts to elicit personal information from you will be quite "legal" as far as your system is concerned, and they are difficult to programmatically detect or prevent. There is no substitute for suspicion with any personal data that is requested from you. Take the following example:


Phishing Email
Westpac Verification Service
Foment C. Pleasure Properties
Customer ID
Password
Sign In
Cancel
mouseover the submit button or link

This email is a live example, received at my home address. On the surface it appears to be a valid request for some information from your bank. Now, clearly, if you are not a customer of this particular organisation you will probably discard the email as a hoax without further consideration.

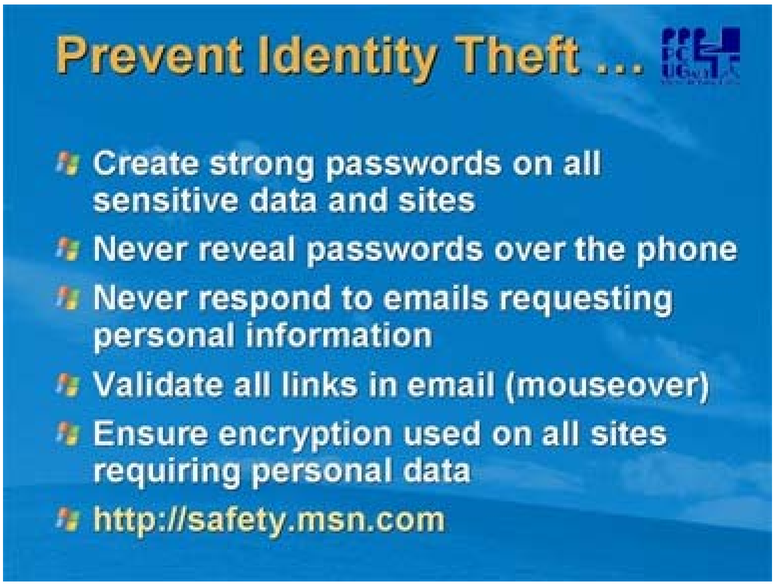
However, think about the case where you are a customer of the bank, and you do have an internet banking account with them. Even if you know all the rules about responding to emails, you might give this a second thought. So let's have a look at why you need to give this sort of communication a wide berth. There are some tell-tell tales that you can use to protect yourself:

Firstly the sender details at the top of the screen. If it really was my bank writing to me, it is far more likely to come from "Westpac Customer Service" than someone with an improbable sounding name. You can of course check the "real" sender by right-mouse clicking on the name, as here, and seeing the correct user and domain name. Not much connection with Westpac here. This isn't foolproof as it is possible for people to "spoof" email addresses – that is make a mail look as if it came from a valid email address when it in fact didn't but this one is obviously not valid. Also check the send date – what bank do you know that sends emails at 2am? That's what I call customer service! Thirdly in the "to:" field it simply has my email name – not even the full address and certainly not my name (or even "valued customer") or similar.

Many of these types of emails have errors in formatting, spelling or grammar. In this case the name of the organisation is misspelt – another giveaway.

However – the one sure-fire method of checking the validity of an email like this is the "submit" or "action" link. As shown here, if you "mouseover" the link or button the real address will be displayed in the status bar at the bottom of the screen. In this case you can see that the address has nothing to do with Westpac and you certainly should not click on the link. If you typed your personal information into this screen your details would have gone to an unknown web site for probable later misuse

The only action you should take with emails like this is to immediately delete them. If you really are concerned that your bank needs personal information from you, then either visit their legitimate site (by keying it into IE directly) or call them. Reputable organisations do not ask for personal information in emails.



Prevent Identity Theft …

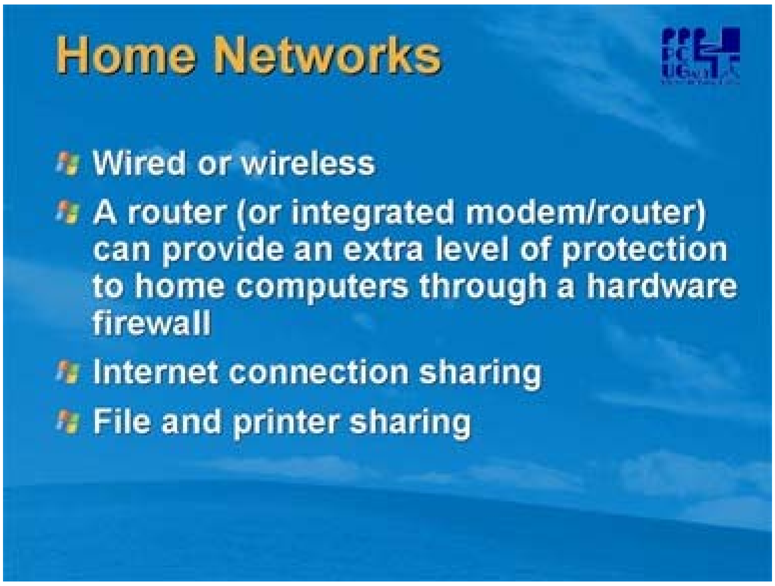
- Create strong passwords on all sensitive data and sites
- Never reveal passwords over the phone
- Never respond to emails requesting personal information
- Validate all links in email (mouseover)
- Ensure encryption used on all sites requiring personal data
- http://safety.msn.com

So what else can you do to prevent this kind of activity? As a simple rule, treat your confidential electronic data as you would your purse or wallet, your passport and other important documents. At least do the following:

- Make sure that you have strong passwords on all sites that you visit that use or display personal data (for example internet banking) and change them regularly. Don't write these down in a file on your computer anywhere
- Don't give your password to anyone for any reason at any time either over the phone or in an email. Period.
- Don't respond to emails asking for personal information. Validate with the requesting organisation that the email is valid.
- At the very least mouseover all links in emails and don't click on them directly
- Ensure the sites you use have encryption in place. The "lock" in the bottom right hand corner is a good indication of this (but not foolproof). Seek advice from the institution if you are concerned. You can check the credentials of the site by double-clicking on the lock

The Microsoft web site safety.msn.com covers more detail on identity theft and is worth a closer look.

Home Networks

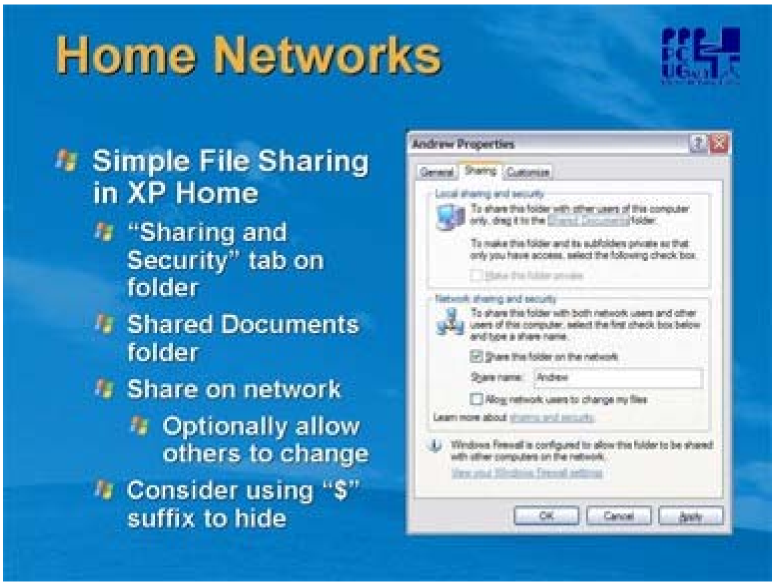


Home Networks

- Wired or wireless
- A router (or integrated modem/router) can provide an extra level of protection to home computers through a hardware firewall
- Internet connection sharing
- File and printer sharing

As discussed previously, one of the best things you can do for your home computer(s) is to hide them behind a hardware router and firewall. Broadband vendors now offer “all-in-one” solutions including such a device, or you can purchase them for around $150 including wireless capability. A router not only provides this protection, it also gives you flexibility in being able to share data and devices between all of the computers in your home. Your home network could be wired (just like your work desktop is, using an Ethernet connection) or wireless. If you go wireless you have additional security considerations, but in Windows XP SP2 these are made easier to manage with the Wireless Network Setup Wizard.

Windows XP also has built-in Internet Connection Sharing, where you can share an internet connection between PCs that are not on a network of their own (for example, two machines that are connected with a crossover cable). This is less common now that home routers are inexpensive and commonplace. We’ll touch a little on file and printer sharing, particularly in a Windows XP Home environment, as it differs from XP Professional and this has some security implications



Home Networks

- Simple File Sharing in XP Home
  - “Sharing and Security” tab on folder
  - Shared Documents folder
  - Share on network
    - Optionally allow others to change
  - Consider using “$” suffix to hide

Andrew Properties

Local sharing and security

To share this folder with other users of this computer only, drag it to the Shared Documents folder.

To make this folder and its subfolders private so that only you have access, select the following check box.

□ Make this folder private

Network sharing and security

To share this folder with both network users and other users of this computer, select the first check box below and type a share name.

☑ Share this folder on the network

Share name: Andrew

□ Allow network users to change my files

Learn more about sharing and security.

Windows Firewall is configured to allow this folder to be shared with other computers on the network.

View your Windows Firewall settings

Both Windows XP Home Edition and XP Professional workstations that are not part of a domain use a network access model called "Simple File Sharing," where all attempts to log on to the computer from across the network use the Guest account. This means that if you're connected to the internet and don't use a secure firewall, your files contained within those shares are available to just about anybody.

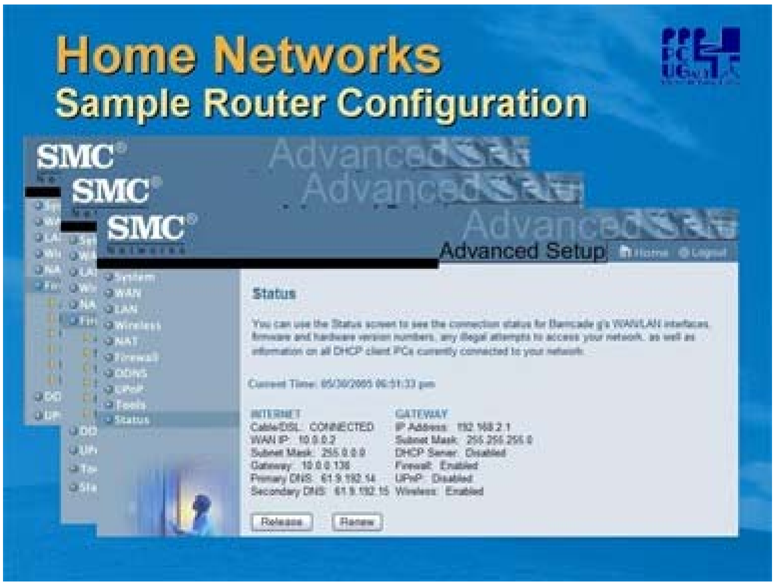
You should ensure, then, that all of your shared folders are read only (don’t check the “Allow network users to change my files” box) and that you share only specific folders and not, for example, the root disk (eg C: or similar). You do have the option to hide the file shares by using a $ sign after the folder name. If you do this users can only gain access to your share if they know its name and connect to it specifically. Microsoft Knowledgebase article KB 304040 details file sharing in Windows XP and is recommended for review.

A word on the “Make Private” option – if you set this for a folder then only you have the ability to access that folder – even other administrative users can’t access it. This is available only to folders in your profile in the “Documents and Settings” folder.

The “Shared Documents” folder is available to all users on the computer by default (you’ll see it in the “My Computer” dialogue) and can be made available across the network as any other share. For the techos out there, the “Shared Documents” folder is actually the “My Documents” folder for the user called “All Users”.

You may need to set an exception in the Windows Firewall if you use file and printer sharing in a home network, to ensure network requests are passed on.

You share a printer in the same way as a folder. You install it on the serving computer, define it as shared and then when you install on other PCs in the network you use the share address.



Home Networks

Sample Router Configuration

Status

You can use the Status screen to see the connection status for Barricade g's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 05/30/2005 06:51:33 pm

INTERNET	GATEWAY
Cable/DSL: CONNECTED	IP Address: 192.168.2.1
WAN IP: 10.0.0.2	Subnet Mask: 255.255.255.0
Subnet Mask: 255.0.0.0	DHCP Server: Disabled
Gateway: 10.0.0.138	Firewall: Enabled
Primary DNS: 61.9.192.14	UPnP: Disabled
Secondary DNS: 61.9.192.15	Wireless: Enabled

We've talked a little about routers and their firewall capabilities. Here are a few screen shots from a standard home router configuration we'll talk about briefly. Each router manufacturer will do this slightly differently, but the concepts are the same. Make sure you familiarise yourself with you router's configuration capability, and if you really don't want to bother with it all, at least allow all the defaults to remain in place.

Make sure that if your router has a password capability you use it – not just the user/password required for the ISP but the firmware password in the device itself

First screen enables the firewall. A very good idea to leave this on even if you do nothing else. You'll find this will stop a lot of hacker activity before it gets anywhere near your PC, and there is no issue in leaving this on AND the firewall in Windows XP for most users.
The next screen is MAC filtering. This is another part of the firewall capability and refers to the ability to limit connectivity to your network to specific devices. All network connect devices (wireless or wired) have a Media Access Control (MAC) address – there is a command line utility you can use to find out yours – and this address is "hard wired" into the device. Filtering devices in this way allows you to control who gets into your network, wired or wireless.

MAC addresses can be trapped by hackers monitoring your network traffic and "spoofed" so this isn't foolproof, but it's a great start.

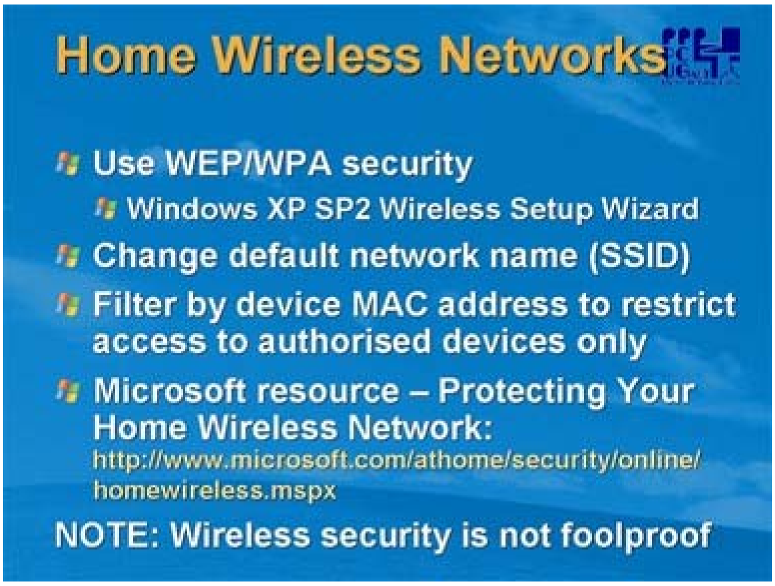
We won't go into the detail of the other options here but if you do have such a device, be sure to review the documentation provided with it to see what other capabilities it has.

The status screen here shows us the effect of a router in our network. In the GATEWAY, it gives us an IP address of 192.168.2.1 (the 192.168 subnet is a default for private networking and this allows easy connection to a Windows network). This is the address of the router on the Local Area Network (LAN) side – the address your PCs need to have set up as the "gateway" to the internet or external network. You set an address in this subnet in each PC you want to configure to join the network – the mechanics for this are outside the scope of the current presentation but we'd be happy to provide more detail after the session.

The GATEWAY address is then mapped (or routed) to the INTERNET address of the router (in this case 10.0.0.2 – this is because in the network setup here there is a modem/router upstream to this device that hides the "real" IP address of the network's connection to the internet). The 10 prefix is a "special"

TCP/IP address that does not provide transport across the internet and is commonly used for “internal” addresses.

Anyway, the message here is that our internal addresses are “protected” by the router, which is also blocking network traffic through its firewall. Not bad for $150.



Home Wireless Networks

- Use WEP/WPA security
  - Windows XP SP2 Wireless Setup Wizard
- Change default network name (SSID)
- Filter by device MAC address to restrict access to authorised devices only
- Microsoft resource – Protecting Your Home Wireless Network: http://www.microsoft.com/athome/security/online/homewireless.mspx

NOTE: Wireless security is not foolproof

What we’ve discussed so far for home networks applies to both wired and wireless networks. It is becoming far more common now for home networks to be wireless, as this means that there are no network cables to be laid and the position of the internet connection point (often the main telephone outlet) is irrelevant when placing equipment.

So what else need to be considered if you go for the wireless option? Like mobile and cordless phones, wireless transmissions are potentially able to be picked up by a third party with the appropriate equipment (which can be purchased cheaply at any electronics store). Thankfully we have some options. The most common of these can encrypt all data on your network using the Wired Equivalence Privacy (WEP) and the later incarnation Wifi Protected Access (WPA) techniques. Windows XP SP2, and most hardware vendors (routers and wireless cards) support both of these. Microsoft strongly recommends their implementation – use WPA if all the devices on your network support it, and WEP if not. The Wireless Network Setup Wizard in SP2 provides an easy way of setting up multiple systems on a home network using either encryption standard.

The difference between the two is that WEP uses a static encryption key and is, in theory, crackable. If a third party can trap enough data on your network they can use certain known fields and other techniques to “crack” this key and uncover your data. In practice the amount of data required is very large and of course the third party has to be in the proximity of your wireless access point or router. However, we do recommend you periodically change the WEP key in all of your devices.

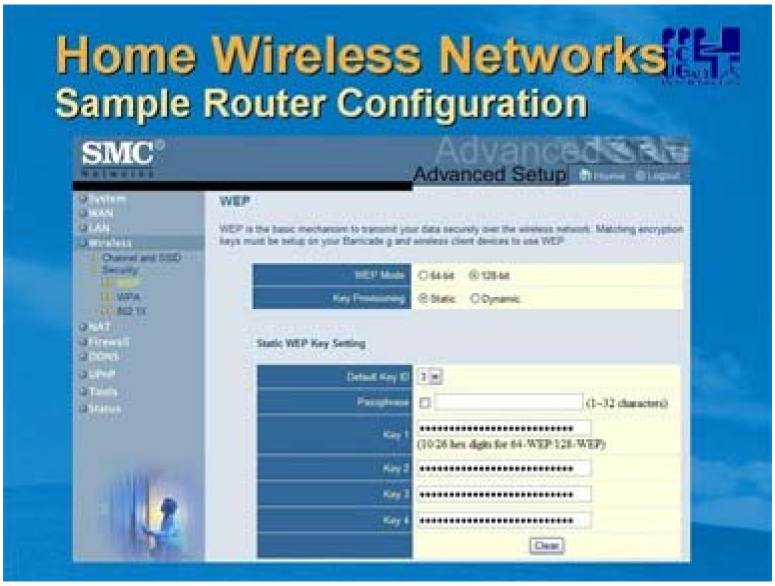
WPA overcomes this by essentially using a “rolling key” that changes frequently. A formal standard (802.11i) is under development to cover this and it is expected that all devices (hardware and software) will confirm in time to this.

The Service Set Identified (SSID) of the network should also be secured – this needs to be known to all devices on the network and should be changed from the default setting in most hardware routers to prevent unauthorised access. Again, this can be circumvented, but it’s going to help keep out some intruders. You can also set this up not to broadcast in a wireless network, so the connecting machine has to know the name of the network to connect.

We’ve already spoken about filtering out devices by their MAC addresses and we recommend that you do this.

There are some standard housekeeping tasks you can perform to keep unwanted visitors from your network – turn the wireless communication point (router or access point) and your computer off when it isn’t being used is a good start.

Before setting up a home wireless network you should be aware of how to make it secure. There are many resources on the internet, including the Microsoft paper referenced here.



Home Wireless Networks

Sample Router Configuration

WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your Barricade g and wireless client devices to use WEP.

WEP Mode: ○ 64-bit ● 128-bit

Key Provisioning: ● Static ○ Dynamic

Static WEP Key Setting

Default Key ID: 1

Passphrase: □ (1~32 characters)

Key 1: •••••••••••••••••••••••••• (10/26 hex digits for 64-WEP/128-WEP)

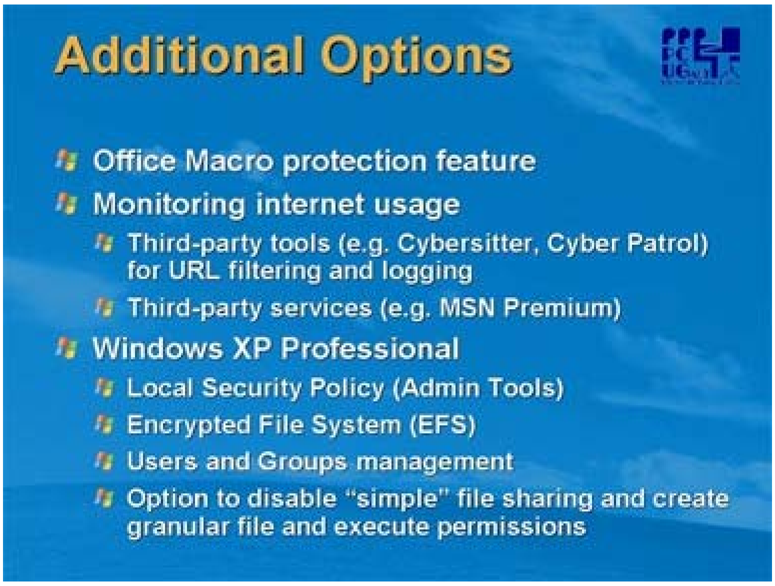
Key 2: ••••••••••••••••••••••••••

Key 3: ••••••••••••••••••••••••••

Key 4: ••••••••••••••••••••••••••

And here’s an example of a router interface to setup WEP encryption. In essence you specify up to four 26-hex digit streams that are used as encryption keys, and select one of these. You then need to set up the same key in each device you want to connect to the network. This particular router supports WPA also, but one of my network adapters doesn’t, so I have to use WEP.

Additional Options



Additional Options

- Office Macro protection feature
- Monitoring internet usage
  - Third-party tools (e.g. Cybersitter, Cyber Patrol) for URL filtering and logging
  - Third-party services (e.g. MSN Premium)
- Windows XP Professional
  - Local Security Policy (Admin Tools)
  - Encrypted File System (EFS)
  - Users and Groups management
  - Option to disable “simple” file sharing and create granular file and execute permissions

So we’ve covered the basic things you can and should do to protect your home computer from illegal attempts to either access it, install software on it or extract your data. There are a few other things we can look at – we won't cover these in detail here but they are things you might like to follow up on if you're interested.

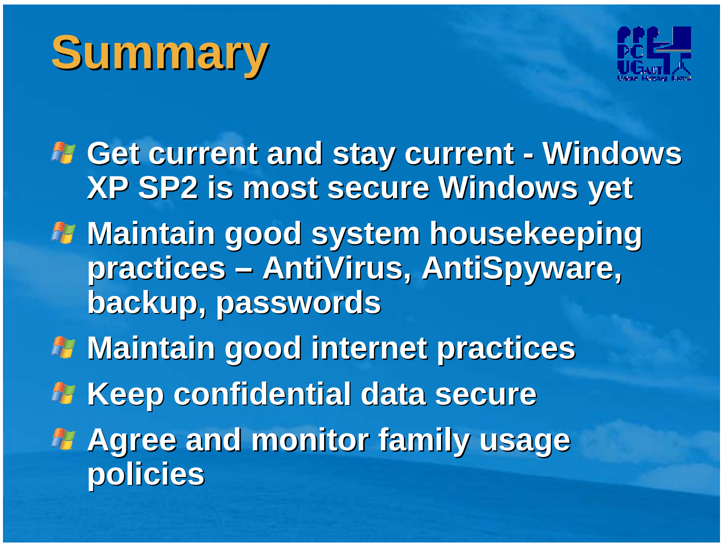
The last couple of releases of Microsoft Office have included "macro protection" – a facility that allows you to protect your system against code written to run in Office programs that you may not trust. Legitimate code can be "signed" and allowed to run, whilst unauthorised code is blocked. This protects you from malicious Office documents that may have hidden code.

If your home PC is used by younger members of your family, you probably already have some kind of monitoring on their internet usage. This can be formalised in a firewall (which can be set up to filter access to the internet) or in third party tools and services that can monitor and control what your children have access to. This is certainly recommended not only because much of the content on the internet is not suitable for children, but also because it can reduce the attack surface available.

If you have Windows XP Professional then you have some other security options not covered in this presentation. If you have one XP Pro system, Microsoft recommends that you use it as the central file, print and internet server (if you don't have a router connection) as it gives you more granular control over system permissions and things like Guest account access).

Specifically, in XP Pro you have Group Policy (which allows the setting of many local security options), the Encrypted File System (EFS) for securing important data; more granular users and groups support and the ability to disable "simple" file sharing and use specific permissions on all files and system resources.

Summary



Summary

- Get current and stay current - Windows XP SP2 is most secure Windows yet
- Maintain good system housekeeping practices – AntiVirus, AntiSpyware, backup, passwords
- Maintain good internet practices
- Keep confidential data secure
- Agree and monitor family usage policies

We hope in the last hour or so we have been able to make you more aware of the things you can and should do to keep your home PC secure. It may seem a bit daunting but there are some key messages here which will keep you in control with minimal effort on your part. So, in short:

- Keep your system current. Most key components (Windows, AntiVirus, AntiSpyware etc) are capable of being updated automatically and should be set to do so.
- Maintain good housekeeping practices. Use passwords, perform regular scans, backup key data, turn your system off when not in use etc
- Maintain good internet and mail practices. Don't open attachments or click links, use website filtering capabilities, use a firewall (hardware or software)
- Keep confidential data secure. Don't give personal data to strangers or in response to emails, use "private folders", ensure websites are correct and secure

Increasingly, system attacks are becoming more sophisticated, and will more increasingly rely on user naivety rather than system weakness to achieve their objectives. Be vigilant and protect your PC as you would your wallet or passport.

I hope the session has been useful to you. Please feel free to spread the message and recommendations to your friends and colleagues.