
By Scott Lowe

Takeaway

Securing Microsoft Windows XP Professional is a must no matter whether the personal computer involved is in a massive enterprise or your home office. This How do I... tutorial walks you through 14 steps that will go a long way toward protecting your Windows XP system from outside attack.

Even though [Microsoft Windows Vista](#) has been out for a while and is available from just about anywhere, most organizations -- at least for the time being -- are sticking with the tried and true [Windows XP](#).

By sticking with Windows XP, these organizations can continue to enjoy XP's stability and familiarity. However, XP users will not be able to take advantage of some of Vista's new security features, such as user access control. But there are a number of steps that can be taken to keep Windows XP running smoothly and securely.

The assumption is that you are using Windows XP Professional, although most of these steps will also work for the Home edition. Most of these steps assume that your Windows XP system is not joined to a domain or that you are in a very small workgroup. Further, although there are dozens of steps you can take to [secure your Windows XP](#) system; these 14 reasonable steps are designed to give you the most bang for your security buck.

Step 1: Give yourself a password

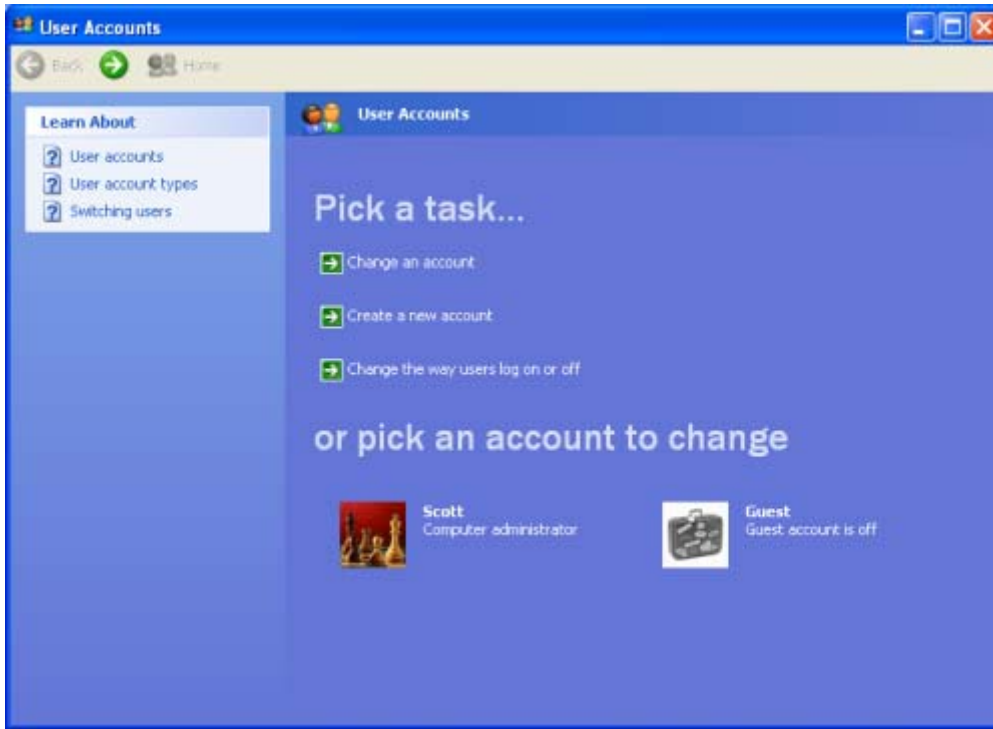
A new Windows XP installation is password-less. That is, when you create the initial account, no password is assigned, but the account has full rights to the machine. Obviously, this is not acceptable in most environments. Even though they can be cracked or stolen, passwords are still the most commonly used security mechanism. Make sure you provide every account with a strong password -- seven or more characters with a combination of upper/lower case, symbols and numbers.

Domain-joined XP clients can change passwords by pressing Ctrl-Alt-Delete and selecting Change Password from the menu. This will change your domain password, which is also your local login password.

To assign a password on a machine that is not joined to a domain:

1. Go to Start | Control Panel.
2. Choose the User Accounts option. This opens the screen shown in **Figure A**.

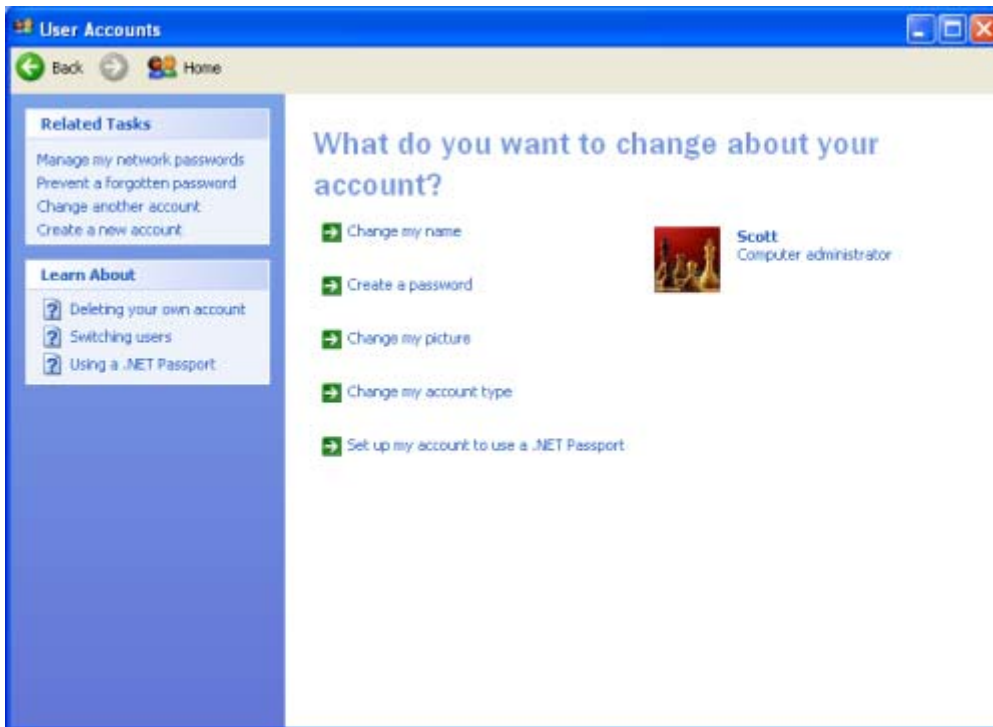
Figure A



The Windows XP User Accounts screen.

3. From this screen, choose the user for whom you would like to establish or create a password. (Figure B)

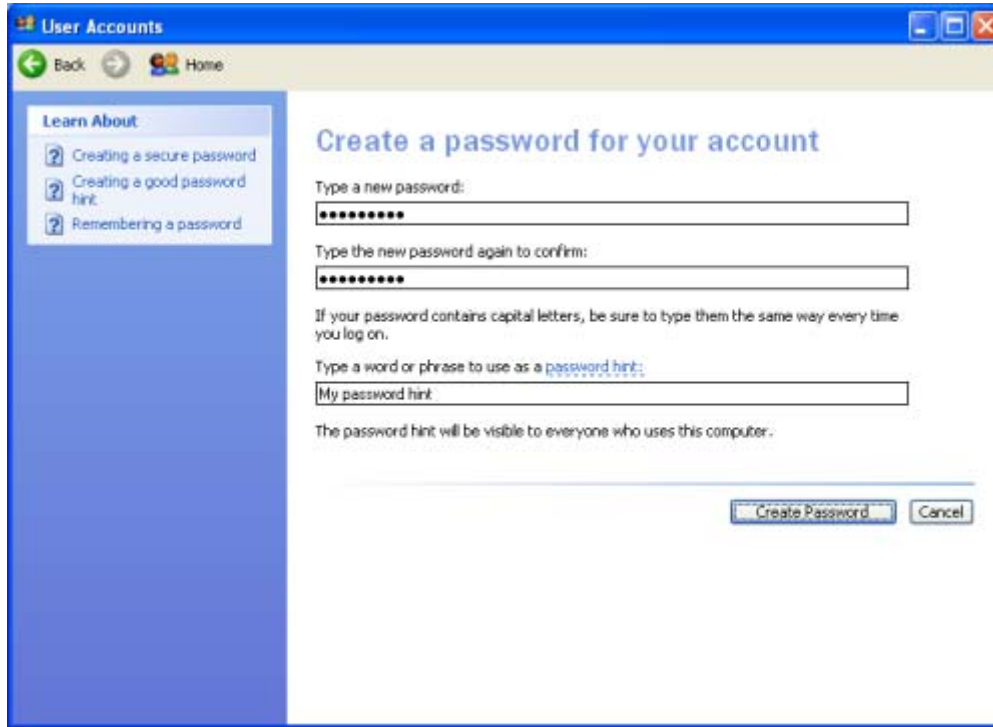
Figure B



What do you want to change about this user?

4. From the resulting screen, choose Create a password. If you already have a password, this option will read Change my password.
5. On the create password window, type the password you wish to assign to the selected user. Optionally, you can also provide a password hint. However, for maximum security, this is inadvisable. If you already have a password assigned to your own user account and you try to change the password, Windows XP will ask that you verify your current password as well. **(Figure C)**
6. Click Create Password button. (or Change Password if you are just changing an existing password)

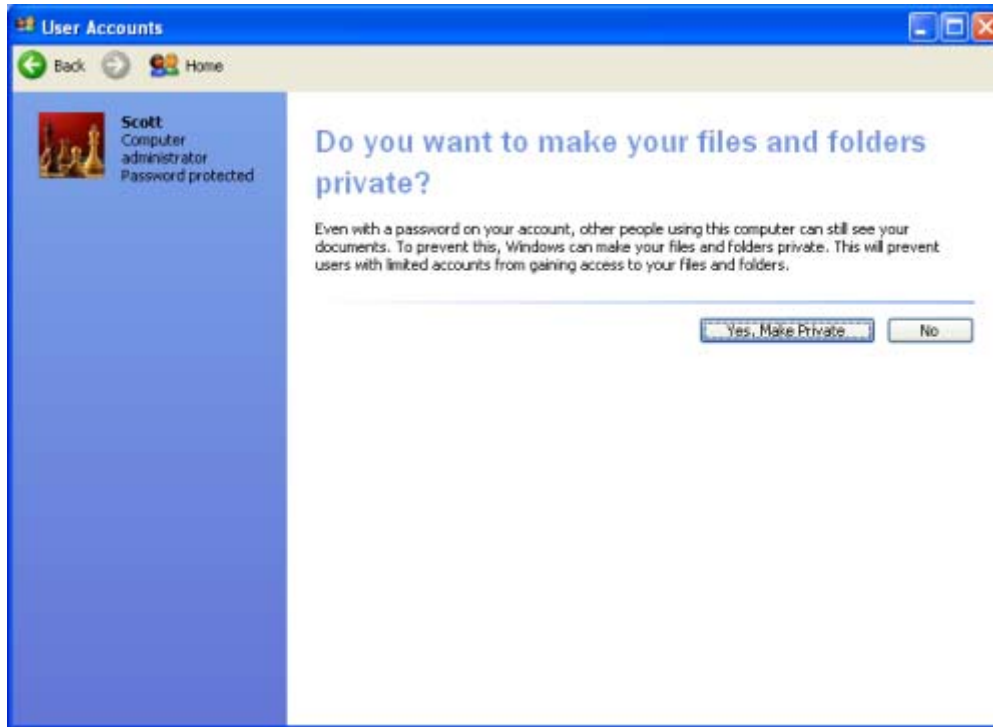
Figure C



Type the password and password hint.

7. Windows XP next asks if you want to make your files private. Windows XP supports administrative and limited access accounts to be created locally. If you would like your files accessible only by those that hold administrative accounts, choose the "Yes, Make Private" button. **(Figure D)**

Figure D



Do you want to make your files inaccessible to limited accounts?

Step 2: Don't run with an administrative account unless necessary

Administrative accounts are the keys to the city, as it were. Mistakes made when logged in as an account with administrative rights can have negative ramifications. For example, as you're browsing various Web sites, if you're running with administrative credentials, spyware can very easily be installed onto your system since there is no barrier between the site and your system.

To prevent, or at least reduce, "drive by" spyware installation and limit damage from viruses, perform your daily tasks as a non-administrative user and only log in as an administrator when you need to install software or perform some administrators-only operation.

Step 3: Apply updates on a regular basis, or use Automatic Update

Patches are a way of life these days. From correcting program crashes to shutting down zero-day exploits, the patch cycle has become integral to staying safe in the online computing world. There are a number of ways that you can go about keeping your system patches current. The easiest method is to make sure that the Automatic Updates feature is enabled.

Follow these steps to check your Automatic Updates status:

1. Go to Start | Control Panel.
2. Choose Security Center.
3. Make sure that the Automatic Updates option is set to On (**Figure E**).

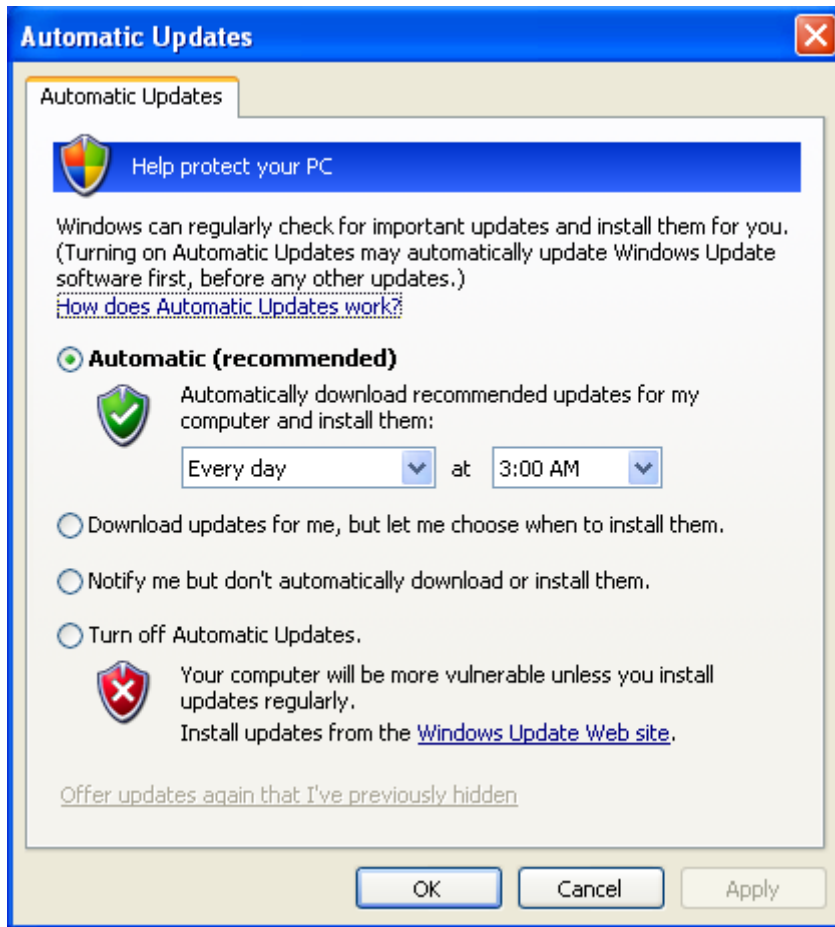
Figure E



The Windows XP Security Center.

If your Automatic Updates setting is Off, click the button marked Turn on Automatic Updates. Besides just enabling Automatic Updates, you can also configure how the feature works. At the bottom of the Security Center screen, click the Automatic Updates option under the heading "Manage security settings for." This will open up the screen shown in **Figure F**.

Figure F



The Automatic Updates configuration window.

From this window, you can make a number of changes in Automatic Updates' default behavior. The default (and recommended) option is Automatic. When you select the Automatic option, you can also decide how often you want to install updates. Your choices are Every Day, Every Sunday, Every Monday, etc. As for times, you can choose any hour of the day that is convenient, but the default selection is to install updates every day at 3 AM. For most people, this will work fine, if the machine is left on for the night.

Your other automatic update options are:

- Download the updates, but install them manually.
- Don't download any updates, but notify the user when new updates are available for download.
- Turn off Automatic Updates altogether. This is not recommended at all.

When you're done configuring Automatic Updates, click OK.

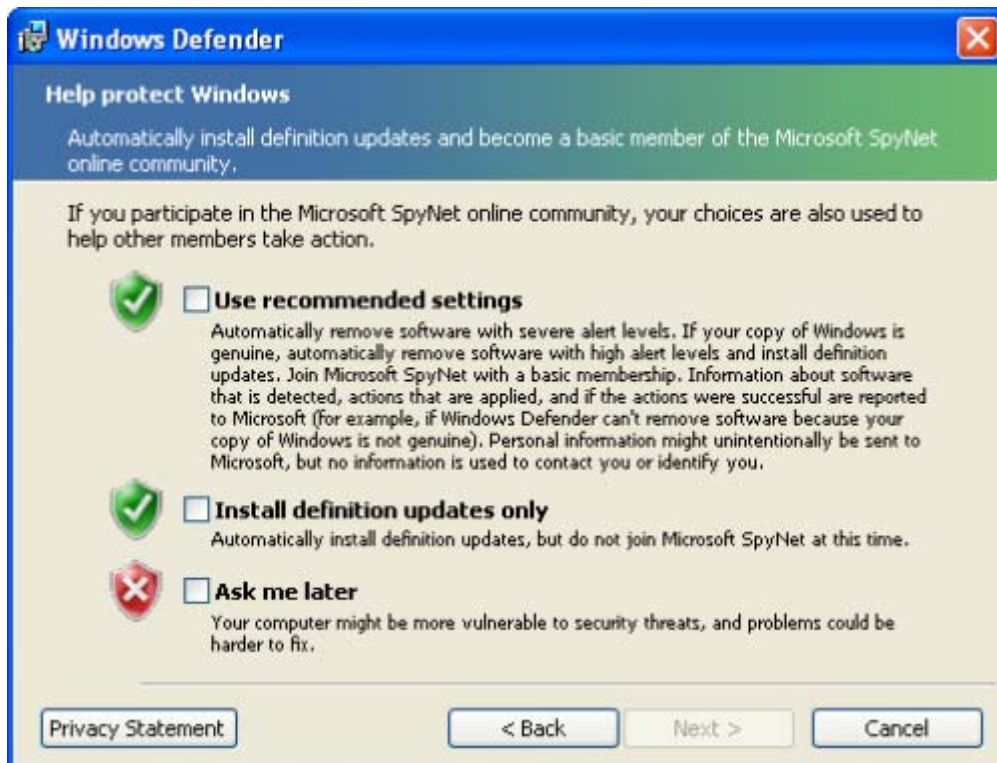
By the way, if you fail to stay current on service packs for Windows XP, you're out of luck on updates. Microsoft is making new Windows updates available only to those that have installed Service Pack 2.

Step 4: Install Windows Defender or another spyware scanner

Windows Defender is actually a very good product, particularly considering its price tag: free. Windows Defender comes standard with Windows Vista. However, Microsoft has made Defender available for [download](#) to Windows XP customers as well. Of course, Defender is far from your only choice when it comes to spyware-busting choices, but since it's free, this is the product I will focus on in this section.

After you download Defender and validate your copy of Windows, you have some decisions to make with regard to the installation. First, decide how Defender should receive updates and take action on particularly harmful spyware. (**Figure G**)

Figure G



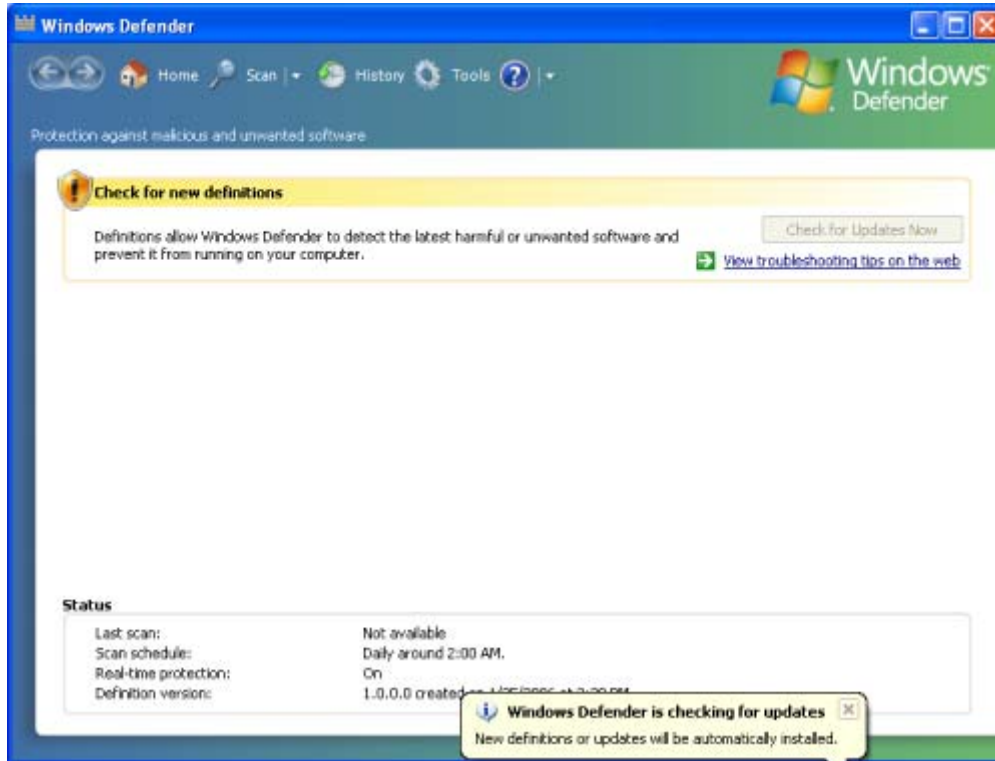
How do you want to update Defender?

There are two update choices from which to choose:

- **Use recommended settings:** The recommended settings for Defender join you to SpyNet (more later) with a basic membership and automatically remove the worst spyware from your system when it is detected. Further, new spyware definitions are automatically downloaded and applied to your copy of Defender. This is the best option you can choose for Defender. SpyNet is actually a good thing as it is basically a community that tracks what actions were taken for a particular piece of spyware. You are then provided a recommended course of action based on what others are doing. However, some personal information transmittal to Microsoft is inevitable so check your organization's security policies before enabling this feature.
- **Install definition updates only:** As the name implies, the only thing that happens automatically is the installation of definition updates. At a minimum, you should select this option.
- You can also choose to make your decision later on.

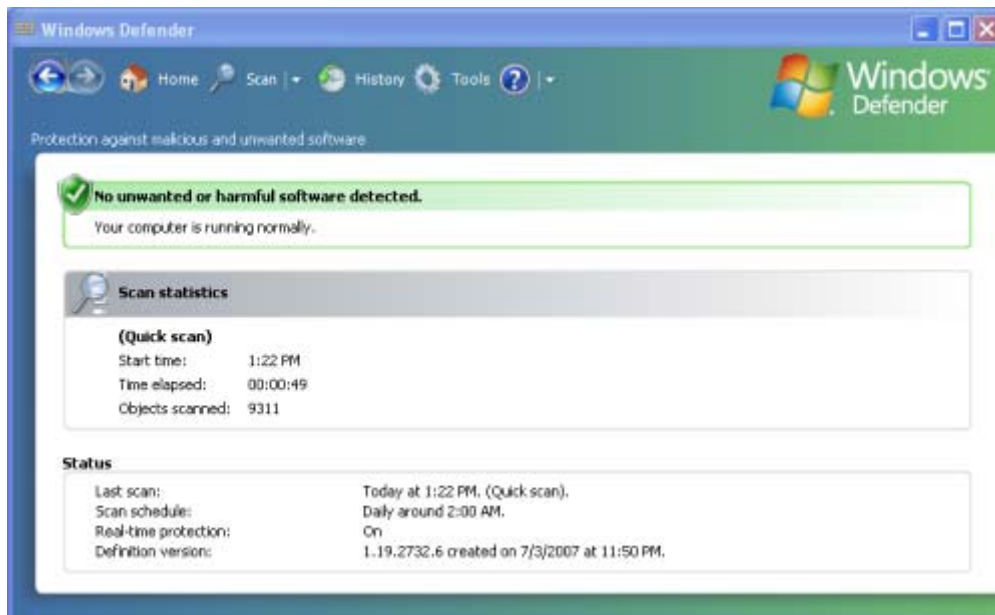
Once you make a selection, the Windows Defender installation completes and Defender starts up, checks for updates, and then performs a quick scan on your system. **Figure H** and **Figure I** give you a look at Defender's initial startup screens. If all goes well, you will have a green bar and no spyware on your system.

Figure H



On Defender's initial startup, an update is performed to get the latest engine and definitions.

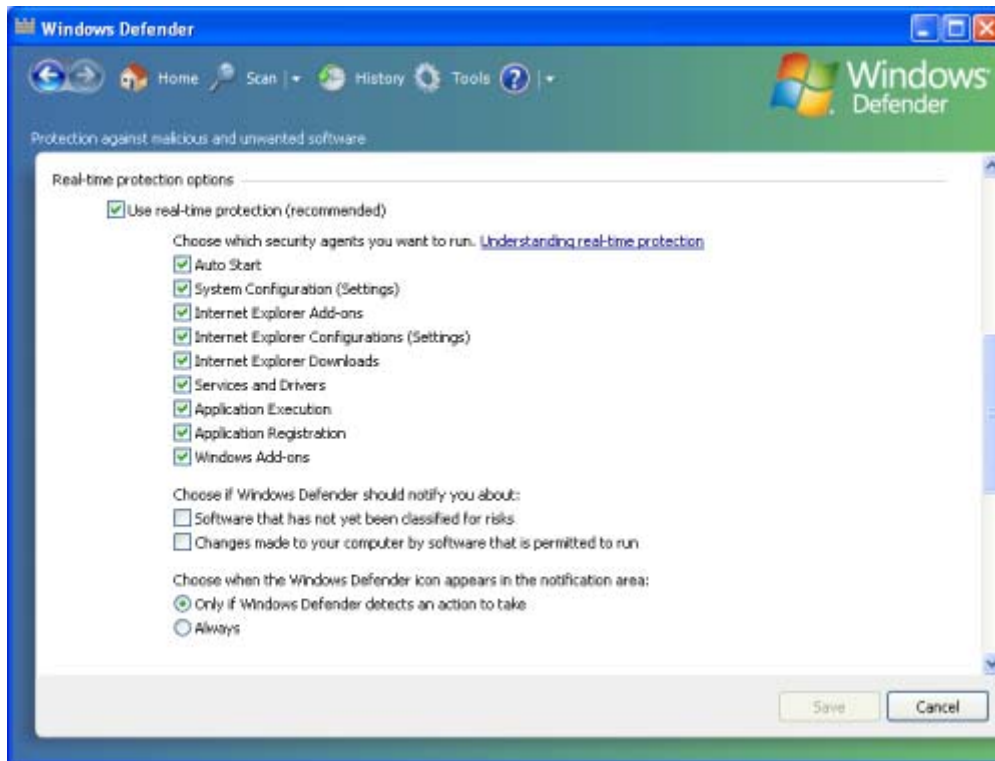
Figure I



The results of the initial spyware scan.

For maximum protection from spyware, regardless of the spyware product you use, make sure you enable real-time protection, like you would in an antivirus product. This proactive scan will help you to catch spyware before it has a chance to actually infect your system. In Defender, go to Tools | Options. Scroll about halfway down the page and make sure that the checkbox next to *Use-real-time protection* is selected along with all of the security agents. (Figure J)

Figure J



Enable all of Defender's real-time security agents.

Even if you use Defender or some other spyware scanning package, you should occasionally use another program like SpyBot to make sure that nothing is missed.

Step 5: Install an anti-virus software package

Although spyware has taken some of the limelight off the difficulties posed by viruses, viruses remain just as much of a threat as they always have. As such, you need to have a good real-time virus scanner. If you don't use Defender for spyware, look for a product that handles both viruses and spyware in one.

Step 6: Use a third party software firewall and a hardware firewall

With XP SP2, Microsoft started shipping a new software firewall that is a huge improvement over versions found in previous editions of Windows. However, for the best in protection, even this new firewall comes up short when compared with third party firewalls. Windows XP's firewall does monitor any traffic originating from your computer. Therefore, you could be spewing all kinds of problematic network traffic and Windows would not block any of it.

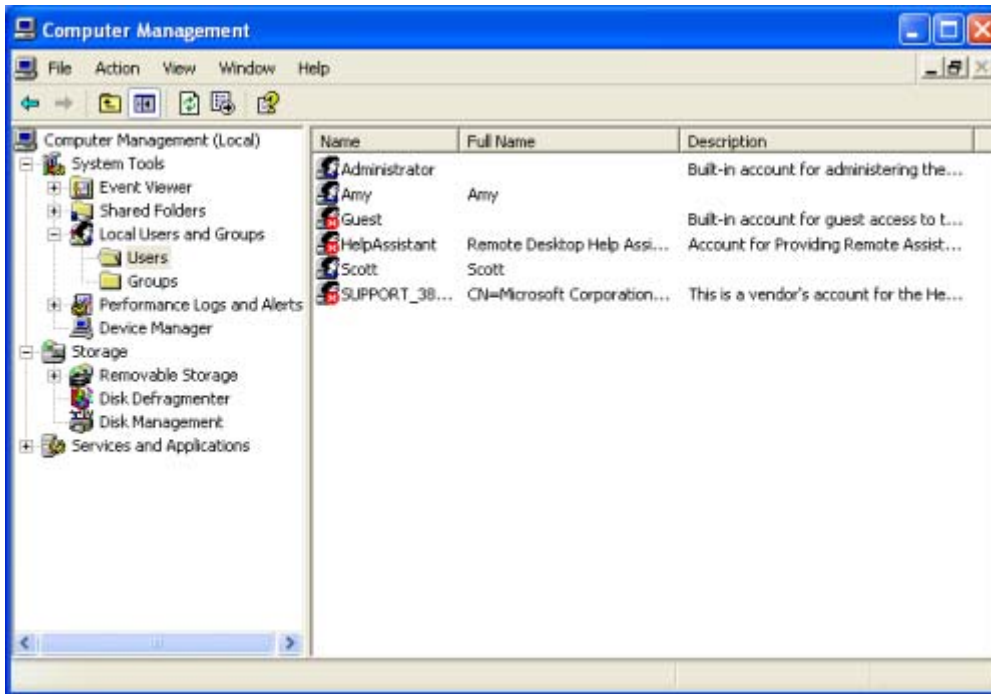
In addition to your software firewall, use a hardware firewall as well. Most corporate networks will have firewalls at the network perimeter, but even if you're in a small or one-person shop, hit your local big box store and pick up a Linksys firewall. Multiple layers of protection from outside threats is one of the best ways to protect yourself.

Step 7: Disable the Guest account

By default in a new Windows XP SP2 installation, the Guest account, which provides limited system access to anyone, is disabled. Verify that this is the case on your system by following these steps:

1. Click the Start button.
2. Right-click My Computer and, from the shortcut menu, choose Manage.
3. When the Computer Management window opens, go to Local Users and Groups | Users.
4. Verify that the Guest account is disabled by looking for an icon with an X in a red circle next to the name. See **Figure K**.

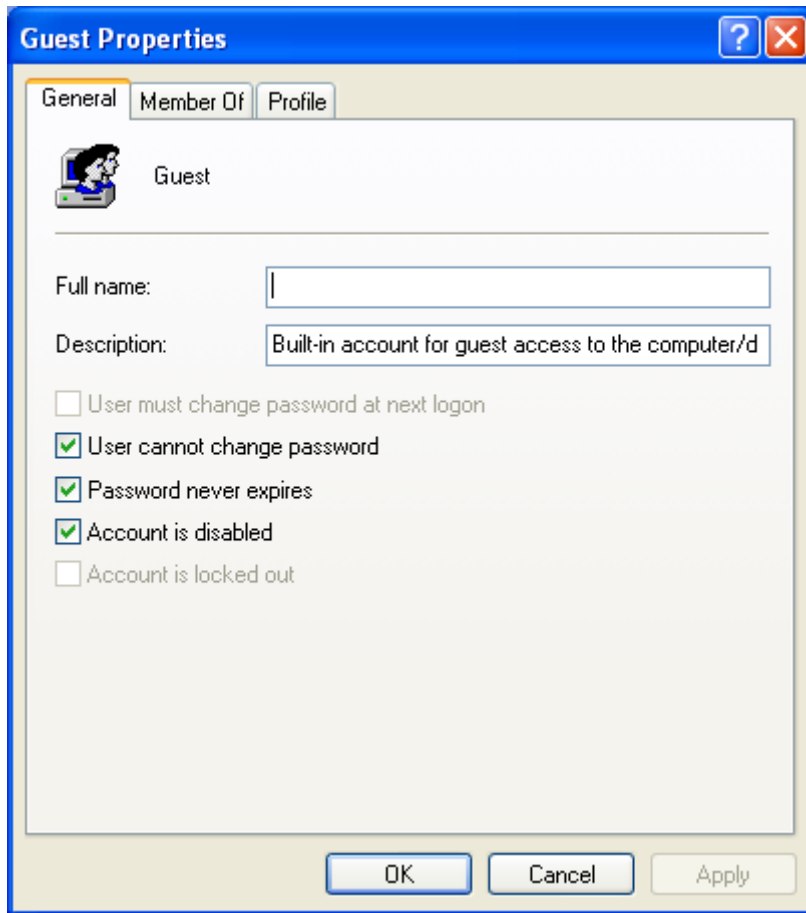
Figure K



The red X next to the Guest account means that the account is disabled.

5. If the account is not disabled, double-click the account name to open its Properties window.
6. On the Guest account's properties window, select the checkbox next to Account is disabled. (**Figure L**)
7. Click OK.

Figure L



This account is disabled.

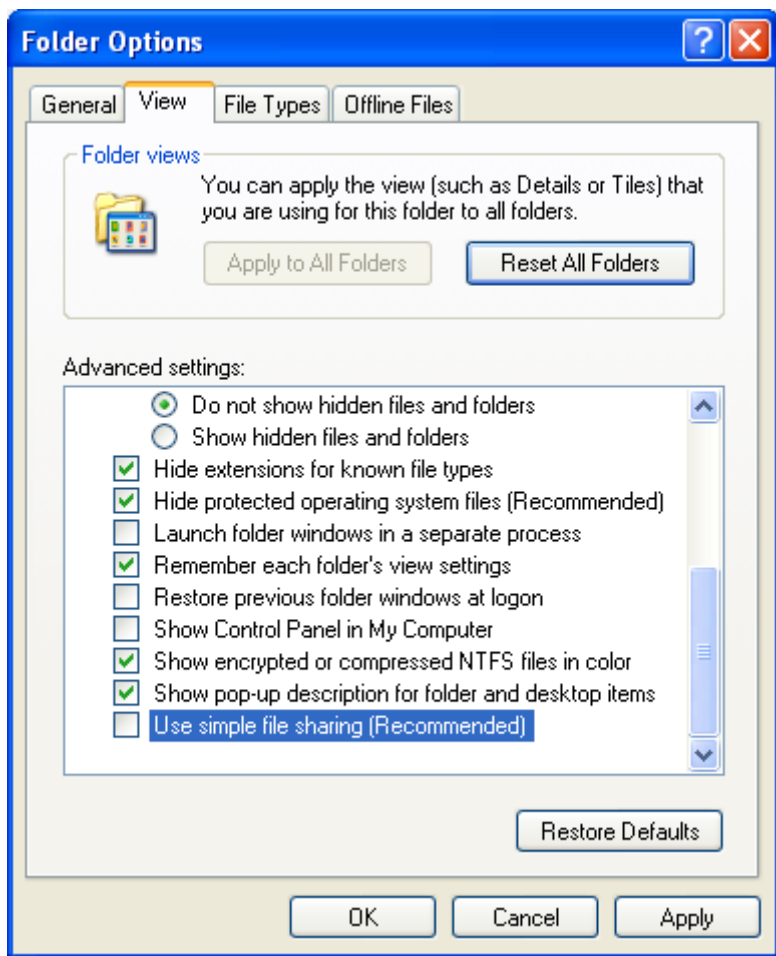
Step 8: Disable Simple File Sharing

Windows XP is designed for both home and office environments. As such, the product attempts to be all things to all people. To make it easier to share files, Microsoft included Simple File Sharing in Windows XP. As the name implies, Simple File Sharing aims to simplify the sharing of files and folders with others. However, with Simple File Sharing, it's an all or nothing proposition. You share your files with everyone or with no one. To better protect your system, disable Simple File Sharing and use Windows' default file sharing method instead. This default method allows you to decide who can access what and at what level.

To disable Simple File Sharing:

1. Go to Start | Control Panel | Folder Options.
2. From the Folder Options window, choose the View tab. **(Figure M)**

Figure M



The Folder Options window.

3. Scroll all the way to the bottom of the advanced settings portion of the window.
4. Deselect the checkbox next to *Use simple file sharing*.
5. Click OK.

Now, when you share files, you can specify who has access to what.

Step 9: Disable unnecessary services

Every service on your Windows XP system performs a function. However, not everyone needs every service. Every running service increases the "attack surface" of your Windows XP system. In short, an unnecessary running service has code running in your computer's memory that could be buggy and could be exploited by others to gain access. So, reduce your computer's attack surface by disabling services that you simply don't need. If you need to know which services are safe to disable and what the ramifications might be for each disabled service, use TechRepublic's [Windows XP Services that can be Disabled](#) spreadsheet.

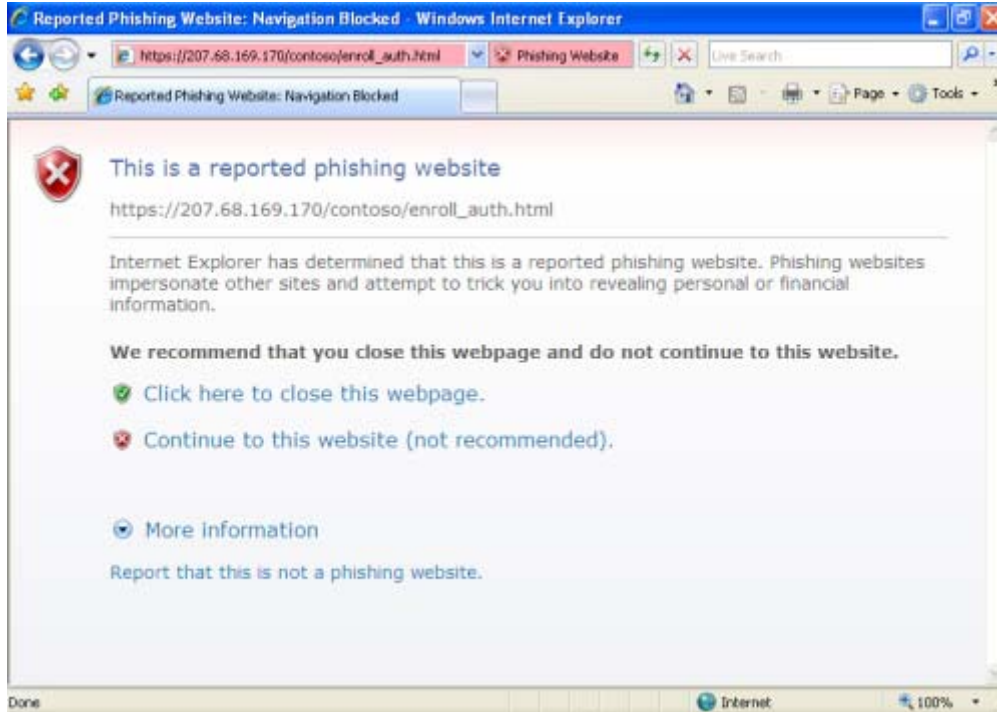
For a look at how to enable and disable Windows XP services, watch [this](#) short video.

Step 10: Upgrade to Internet Explorer 7

Internet Explorer is widely considered to be the most insecure browser out there. Internet Explorer 7 aims to correct some of the product's shortcomings. IE 7 is available through Automatic Updates, and is also available for [download](#) from Microsoft. IE 7 includes these new features that help to protect your system:

- A phishing filter: Helps to avoid accidentally giving your personal information away to criminals. When you browse to a known phishing site, the address bar turns red and IE7 informs you that the site is listed as a phishing site. (Figure N)

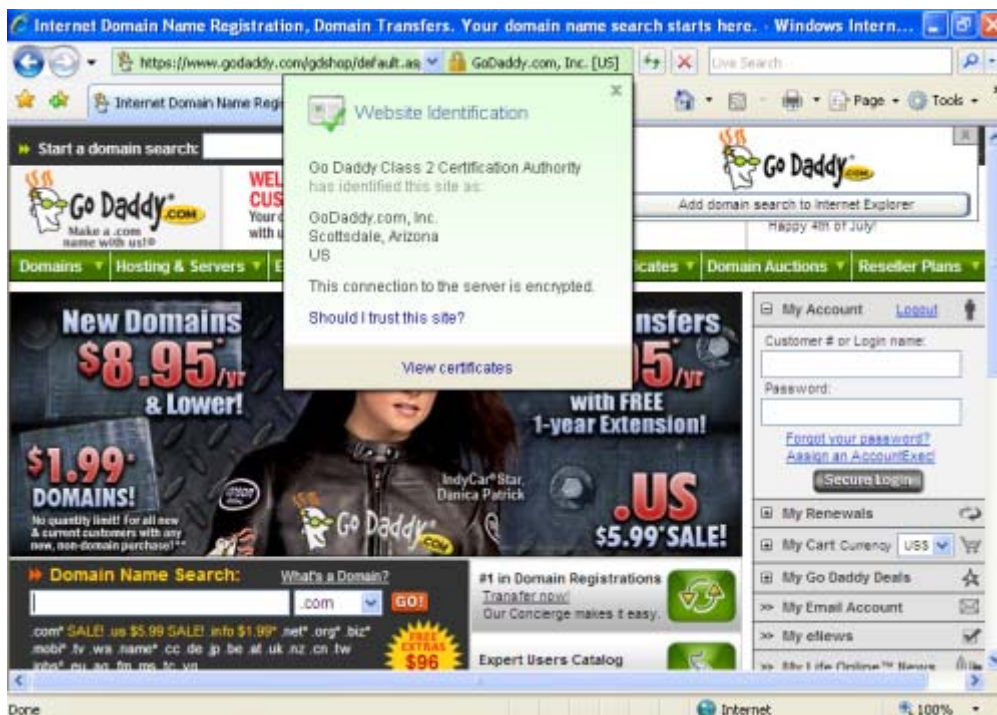
Figure N



This site is on the list of phishing websites to avoid.

- Cross-domain barriers: IE7 helps to prevent scripts from interacting with content in other places, giving you additional protection against spyware.
- Visual security tips: I mentioned the phishing filter's ability to let you know when you've visited a phishing web site. In addition, when you visit a site that is particularly well protected (through the use of an extended validation [EV] certificate), the address bar turns green letting you know that the site is safe. (Figure O)

Figure O



An Extended Validation certificate in action in IE 7.

These are just some of the major security improvements found in IE7. If you have not, you should upgrade ASAP.

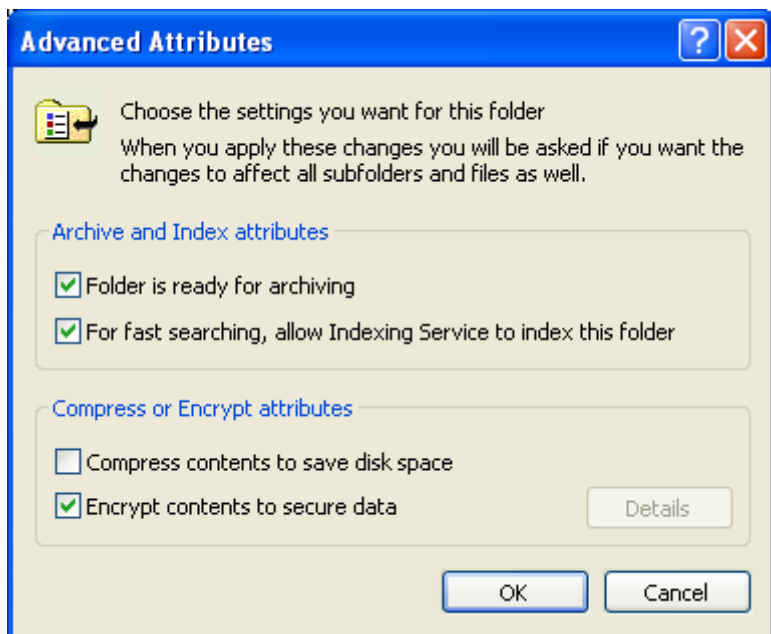
Step 11: Encrypt whatever you can

A username and password combination is a good beginning to protecting files and folders. However, if a machine -- particularly a laptop -- is stolen it's a very simple matter to break into the contents of the hard drive. The only way you can be reasonably sure that files and folders will remain inaccessible to a thief is to encrypt files so that they are extremely difficult to pry open.

Windows XP includes the ability to selectively encrypt files and folders. To do so:

1. Right-click the folder that contains files that you want to encrypt.
2. From the shortcut menu, choose Properties.
3. On the General tab, click the Advanced button.
4. Select the checkbox next to *Encrypt contents to secure data*.
5. Click OK. (Figure P)

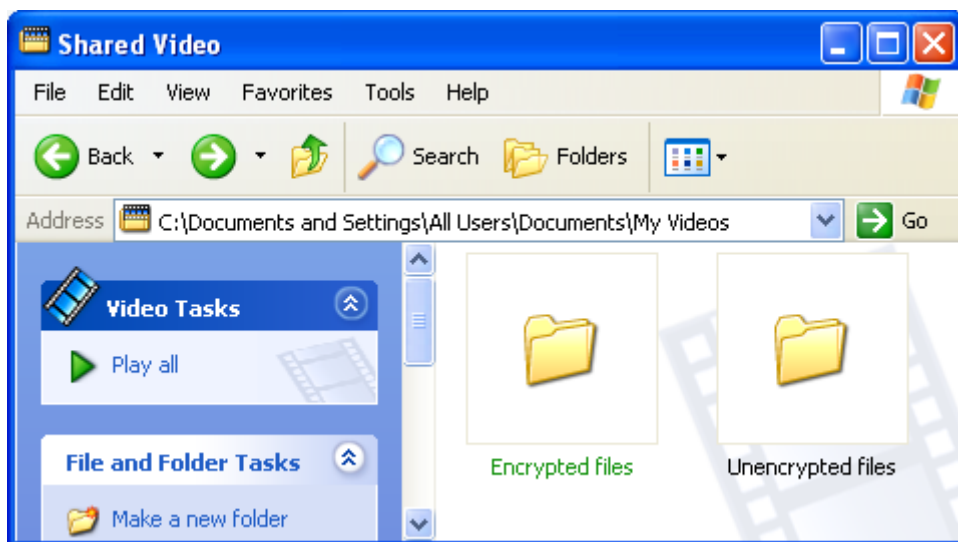
Figure P



The contents of this folder will be encrypted.

When you encrypt a file or folder, that item's title becomes green, as shown in **Figure Q**.

Figure Q



Encrypted folder titles are green.

You should, at a minimum, encrypt the Temp folder since copies of any documents you are working in can reside here.

Consider whole-disk encryption

For laptop users, an even better option than XP's selective encryption is whole disk encryption. Although these products can result in a performance hit, if you have sensitive information of any kind, you simply can't afford *not* to have the information encrypted. Full-disk encryption means that it doesn't matter where you store your files; they'll always be protected.

Step 12: Always use NTFS

These days, there is almost no reason to *not* use NTFS. FAT and FAT32 are supported in Windows XP, but are not nearly as flexible as NTFS, nor are they as secure. Nor do FAT and FAT32 allow for partitions as large as those allowed by NTFS. For all of these reasons, you should use NTFS whenever possible. If you have a Windows XP system running with FAT or FAT32, you should convert the non-NTFS partitions to NTFS.

To do so, from a command line, use the command:

```
convert (drive letter) /fs:ntfs
```

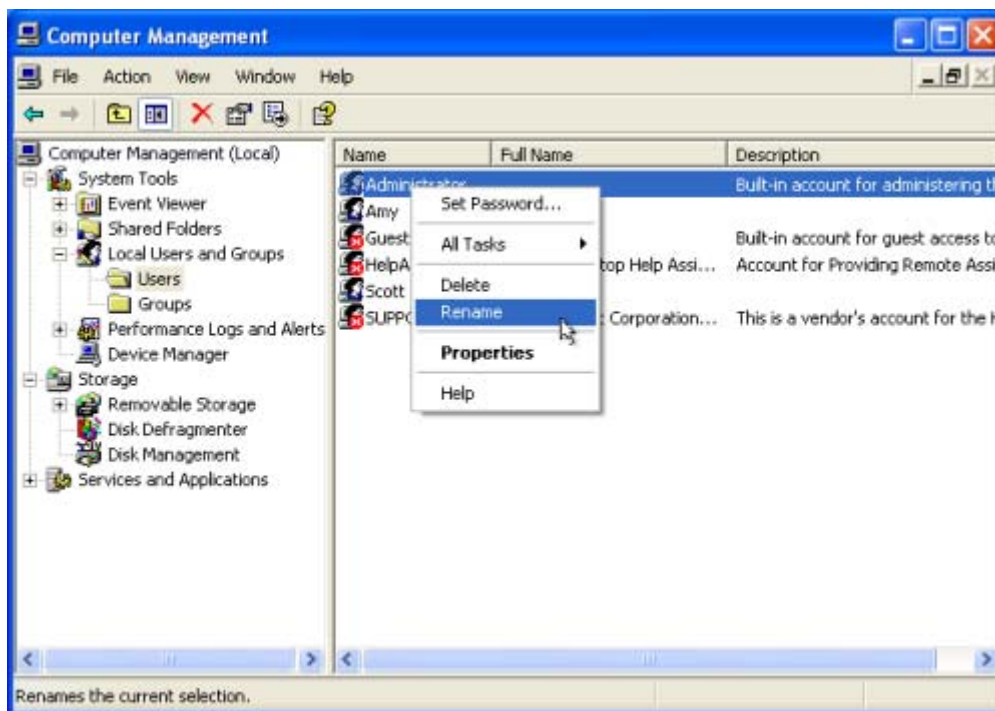
This is a one way transition.

Step 13: Rename the Administrator account

Every Windows XP installation has an Administrator account. Although a hacker can use other methods to obtain the name of the primary administrative account, by renaming this account to something else, you make it that much more difficult for them. To rename the Administrator account:

1. Click the Start button.
2. Right-click My Computer and, from the shortcut menu, choose Manage.
3. When the Computer Management window opens, go to Local Users and Groups | Users.
4. Right-click the Administrator account and, from the shortcut menu, choose Rename.
5. Type the new name you want to use for the Administrator account. (**Figure R**)

Figure R



Rename the Administrator account.

As an additional step, you could also create a dummy account named Administrator that actually has no rights on the system. Again, this will not deter determined hackers, but is another wall you can throw up on their trail.

Step 14: Use Group Policies whenever possible

Group policies provide a large number of security options and make it easy to secure all of the Windows XP computers in your organization in one fell swoop. Learn everything possible about Group Policy and then use this feature to secure your organization. Visit Microsoft's [Windows Server Group Policy site](#) for tutorials, information and labs related to Group Policy.

Summary

These 14 steps will go a long way toward protecting your Windows XP system from outside attack. While there are other things that you can do, these techniques are a step in the right direction.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) [XML](#)
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for TechRepublic's [Windows XP](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)
- Catch up with all the [How do I](#) articles on TechRepublic.

Version history

Version: 1.0

Published: July 12, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team