

Computer Security Tutorial

This tutorial was created by Seager Enterprises on October 4, 2007 using a Dell Computer with Windows XP Professional in Windows classic mode and Microsoft Word 2003. Internet Explorer 6 is used for the Internet examples.

The tutorial will discuss the main phases of computer security including the following:

1. Windows Firewall
2. User Accounts
3. Windows Passwords
4. Windows Security Center
5. Internet Security – Security & Unsafe

Each area will be discussed in detail. To navigate this tutorial, hold down the CTRL key and click with the mouse to move from section to section.

The Table of Contents will follow.

Table of Contents

Windows Firewall.....	2
User Accounts	3
Windows Passwords.....	10
Windows Security Center	12
Automatic Updates.....	12
Anti-Virus Protection	13
Internet Safety & Protection.....	14
Recognize phishing scams and fraudulent e-mails	14
What does a phishing scam look like?	14
How to tell if an e-mail message is fraudulent.....	15
Use the latest products & services to protect you from online scams	16
Smart Downloading with Internet Explorer 6	16
Should I Save or Open?.....	16
What Internet Explorer 6 Does.....	17
Improvements to Internet Explorer 6 with Windows XP SP2.....	18

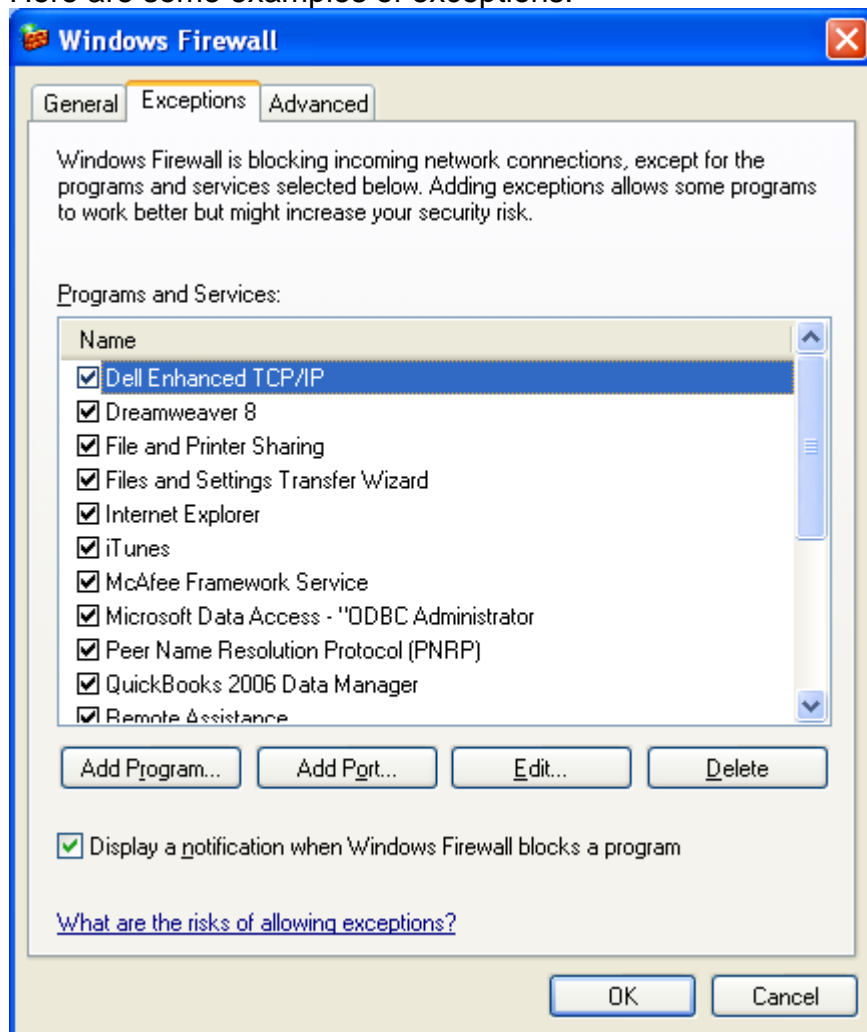
Windows Firewall

The Windows Firewall is the primary safeguard for your computer. It contains protection for those using the computer from outside sources. The firewall blocks “hackers” from penetrating the files on your computer. You can actually manipulate who can access and who cannot the files on your machine. (NOTE: to return to Windows Security Center section, click [HERE](#))

As an example, you have installed a program that requires updates. Most of the time, the firewall accepts the website that supports the program and places an “exception” link within the firewall.

To reach the windows firewall, click on Start, then Settings, then Control Panel and finally Windows Firewall.

Here are some examples of exceptions:



Many of the programs shown here require updates and some are inherent within the operating system itself.

Notice that you can: Add Programs, Add Ports (Channels) edit the list and delete entries. Be careful that you do not accidentally delete or add programs or ports for which you are unsure.

To be safe, leave the firewall ON.

[RETURN TO TOP](#)

User Accounts

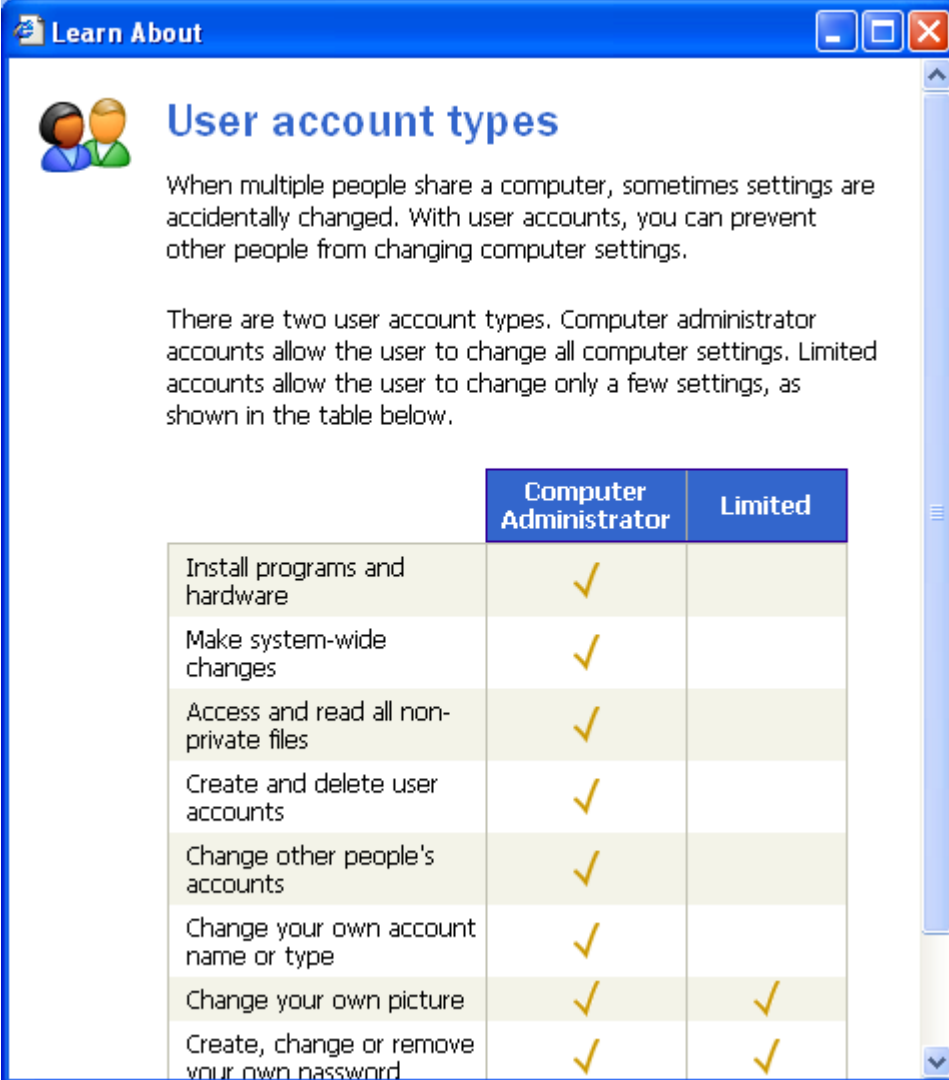
A user account is the area where individuals can create “profiles” or settings unique to each person who wants to use the computer. Each user can have their own account and protect all settings by creating a **password** to keep others from accessing personal and confidential information and settings.

To reach the user accounts, click on Start, then Settings, then Control Panel, and then User Accounts.

With Windows XP there is an account that is usually hidden called an “Administrator” account. In an Administrator account, you can create other administrator accounts. Administrator accounts give a user full access to all files and settings in their account. This is important when installing or updating the computer or programs, etc.

You can also bypass this method by going to the User Accounts in the Control Panel to see if you, as the present user, have an administrator account. It will show it next to the user name that is visible. The other type of account is called a Limited Account. There is also, by default, another account called a Guest Account.

The differences between an Administrator accounts and Limited accounts are these:



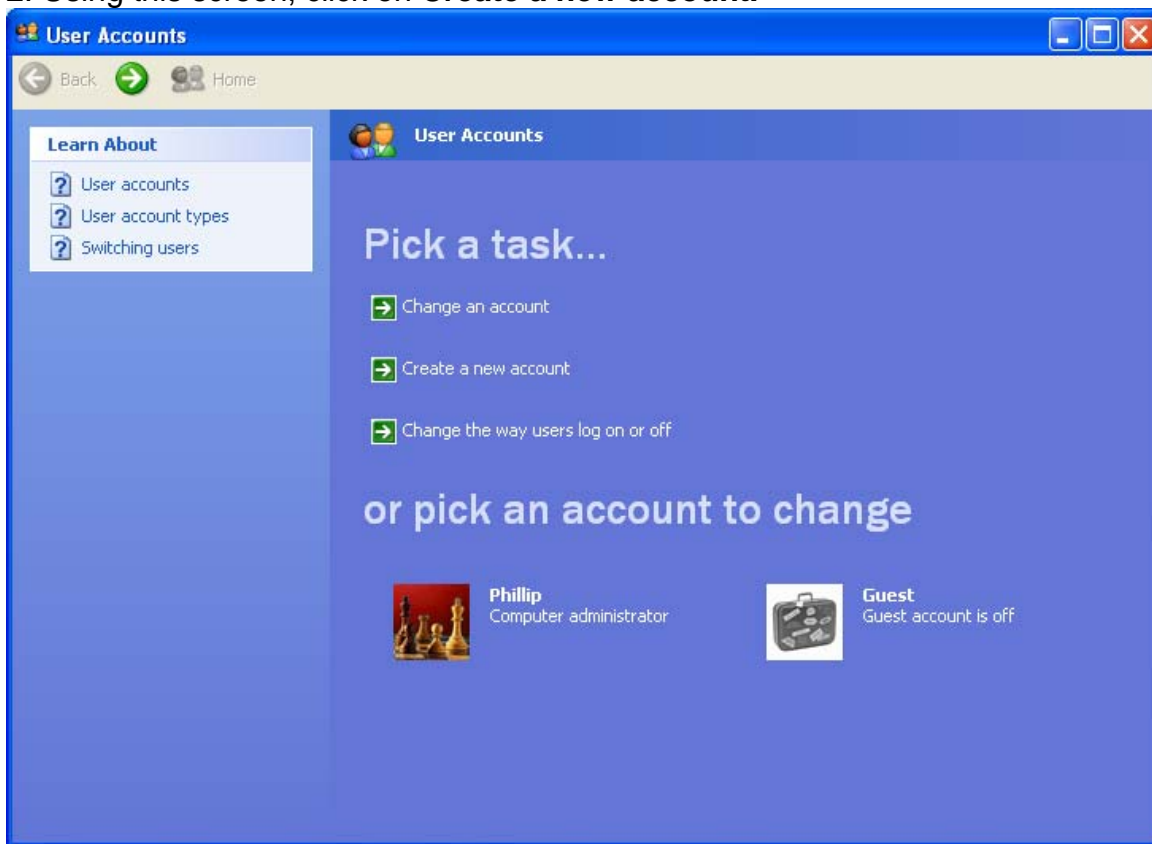
User account types

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

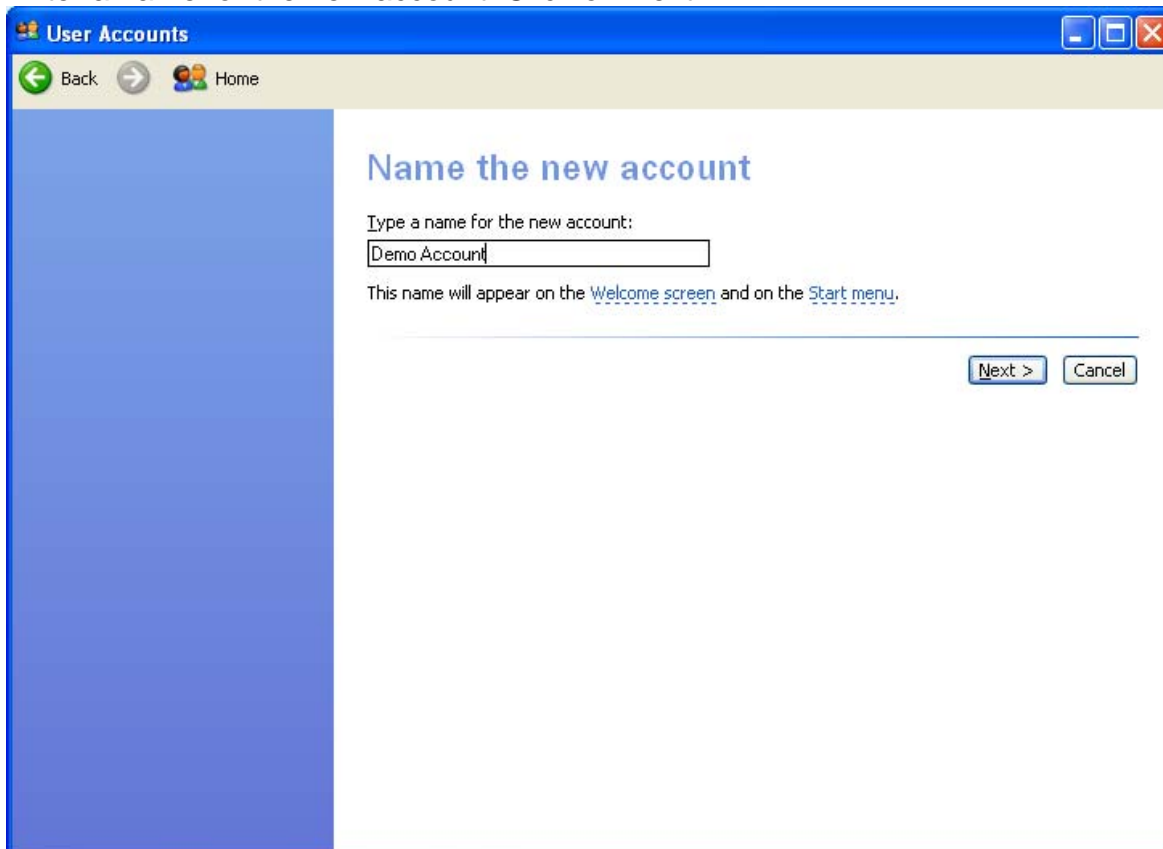
There are two user account types. Computer administrator accounts allow the user to change all computer settings. Limited accounts allow the user to change only a few settings, as shown in the table below.

	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	✓	✓

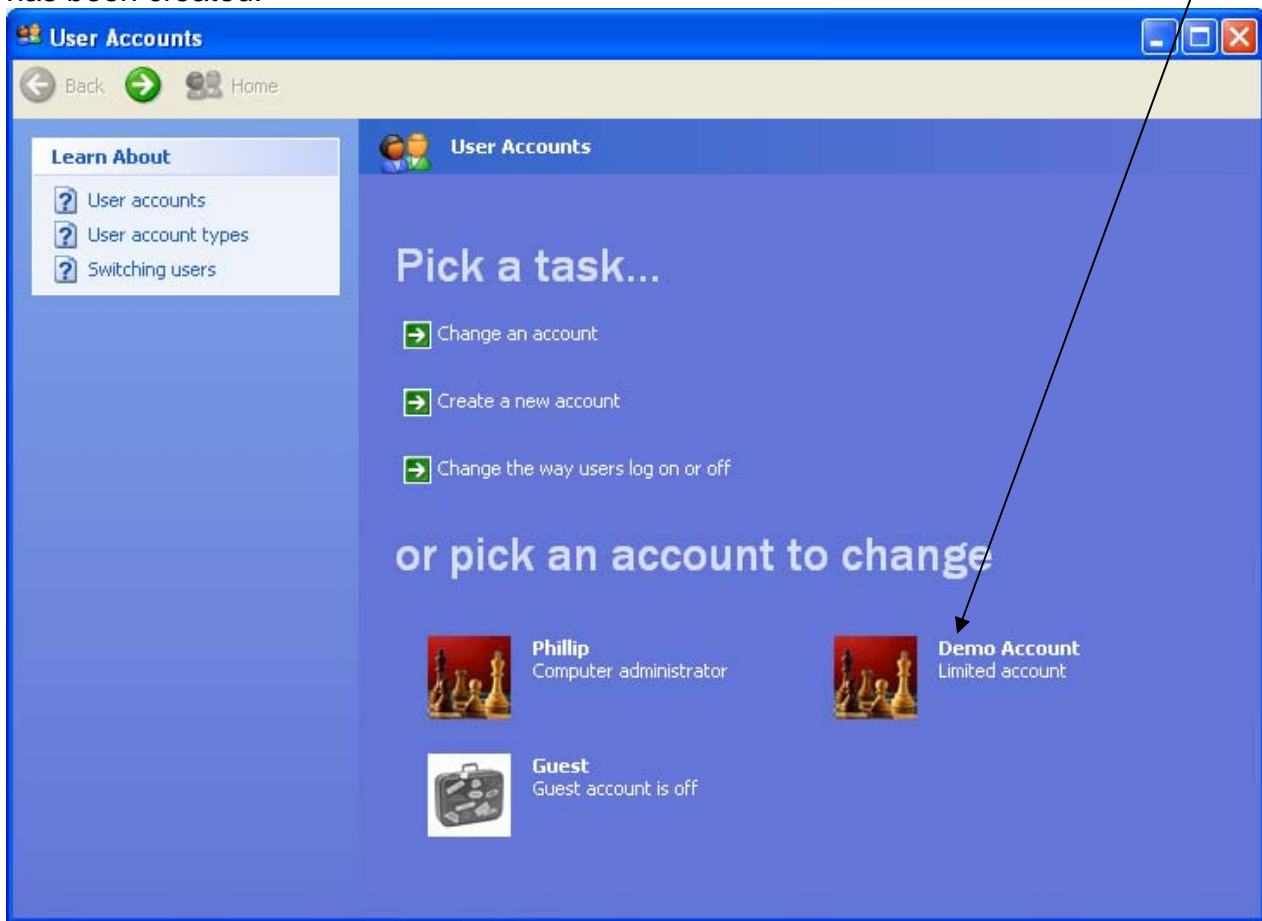
- To set up an account, either as Computer Administrator or Limited you must follow these steps:
1. Click on Start, then Settings, then Control Panel, and then User Accounts.
 2. Using this screen, click on **Create a new account**.



Enter a name for the new account. Click on Next.



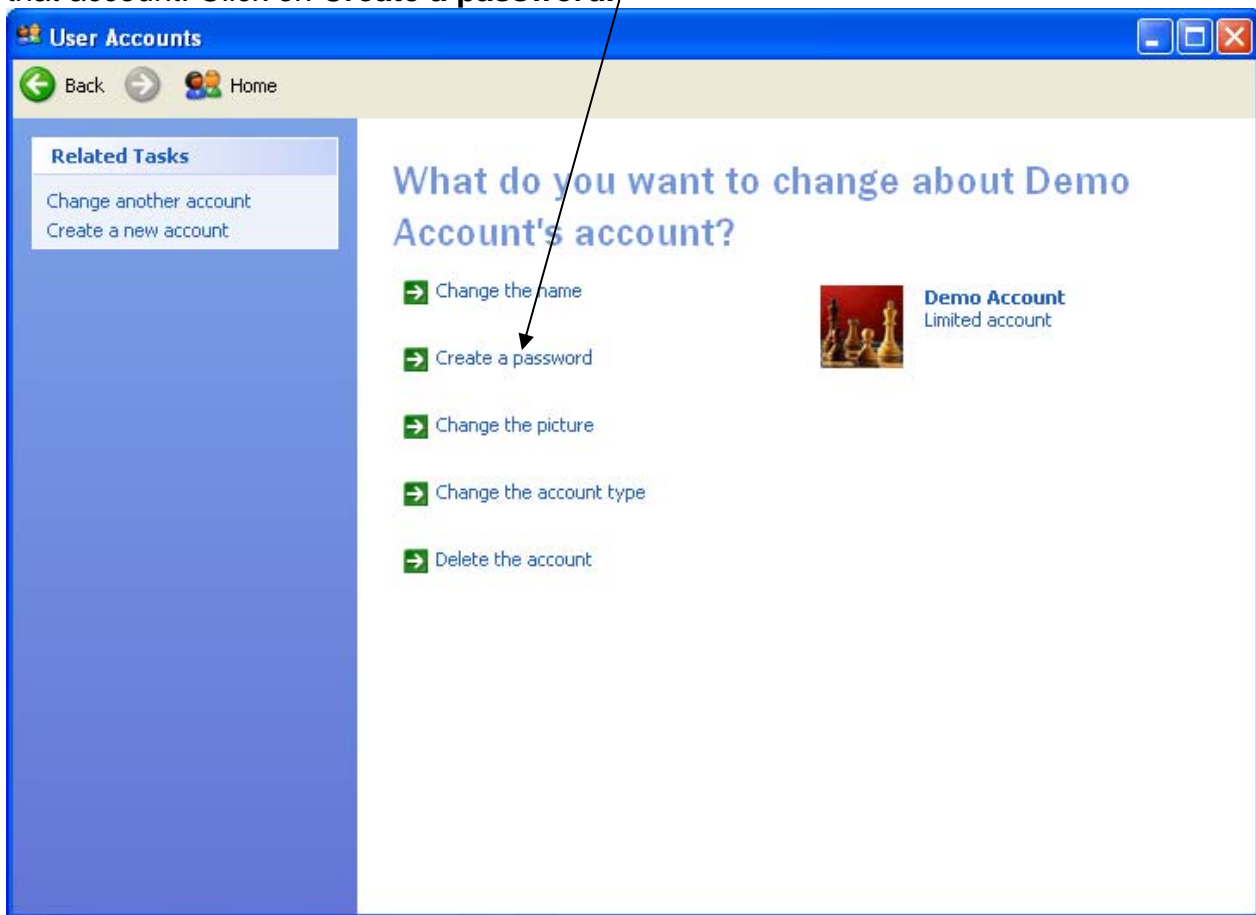
Determine which type of account you want it to be. If you are a parent, and you are creating this for a child, choose the Limited one. For this tutorial, that will be our selection. The new account has been created.



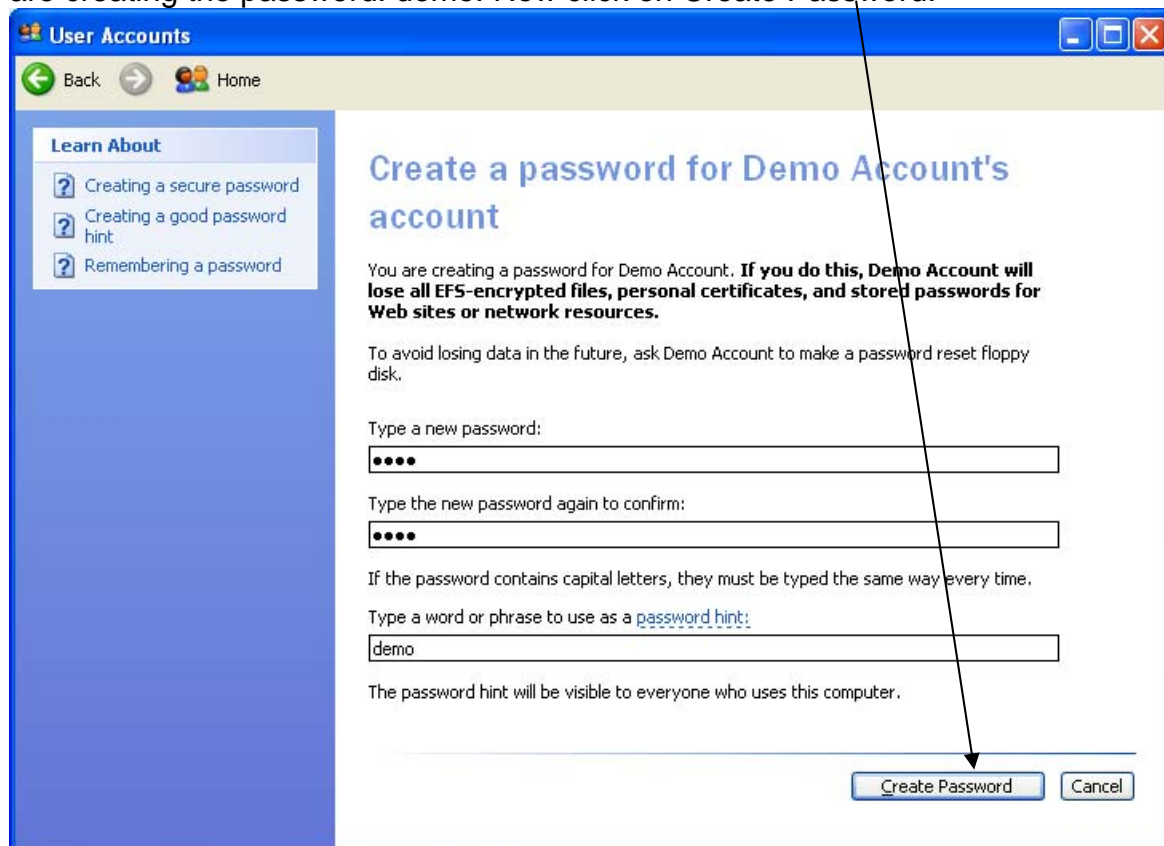
Computer administrators have the rights to change the account type and also to delete the account.

Each user has the right to create a password and a new picture. To do this, click on the account where you want to either create a password or change the picture. We will do the demo in this lesson.

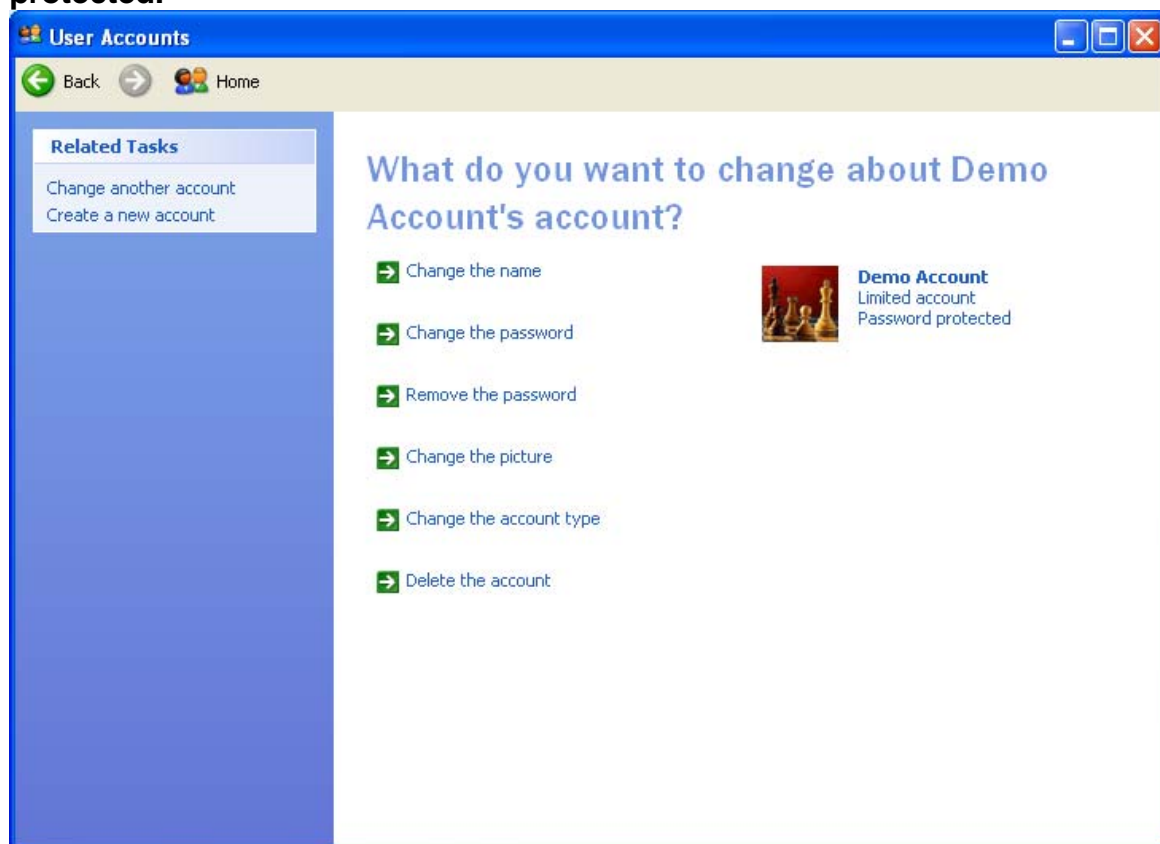
Click on either **Create a password** or **Change the picture**. From our earlier notes, we know that Limited users cannot Change the account type or Delete the Account when logged on to that account. Click on **Create a password**.



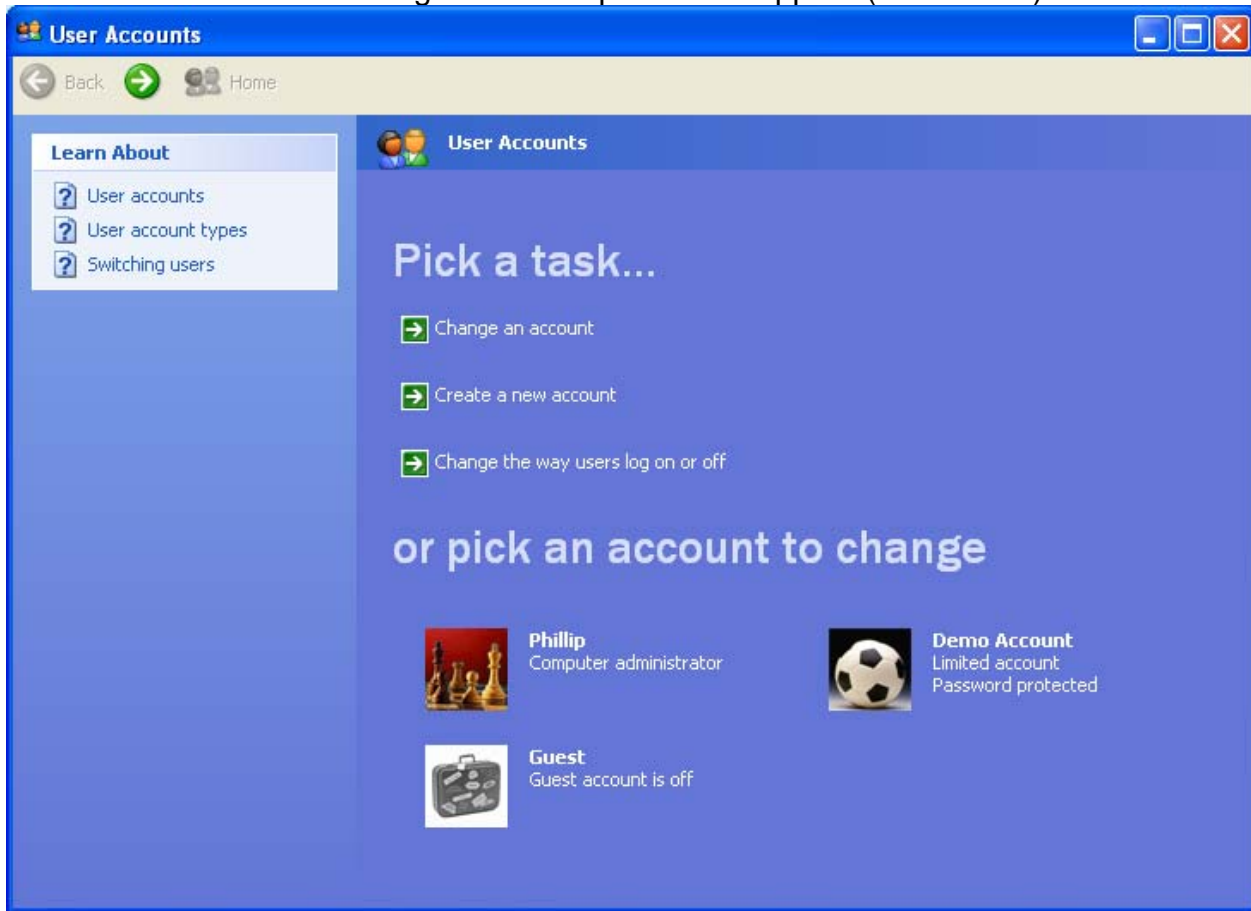
Read the information presented here, then type in a new password, then do it again in the box below and then put in a password hint that will help in case you forget the password. Here we are creating the password: demo. Now click on Create Password.



You will now return to the main screen. This screen will show that the account is **password protected**.

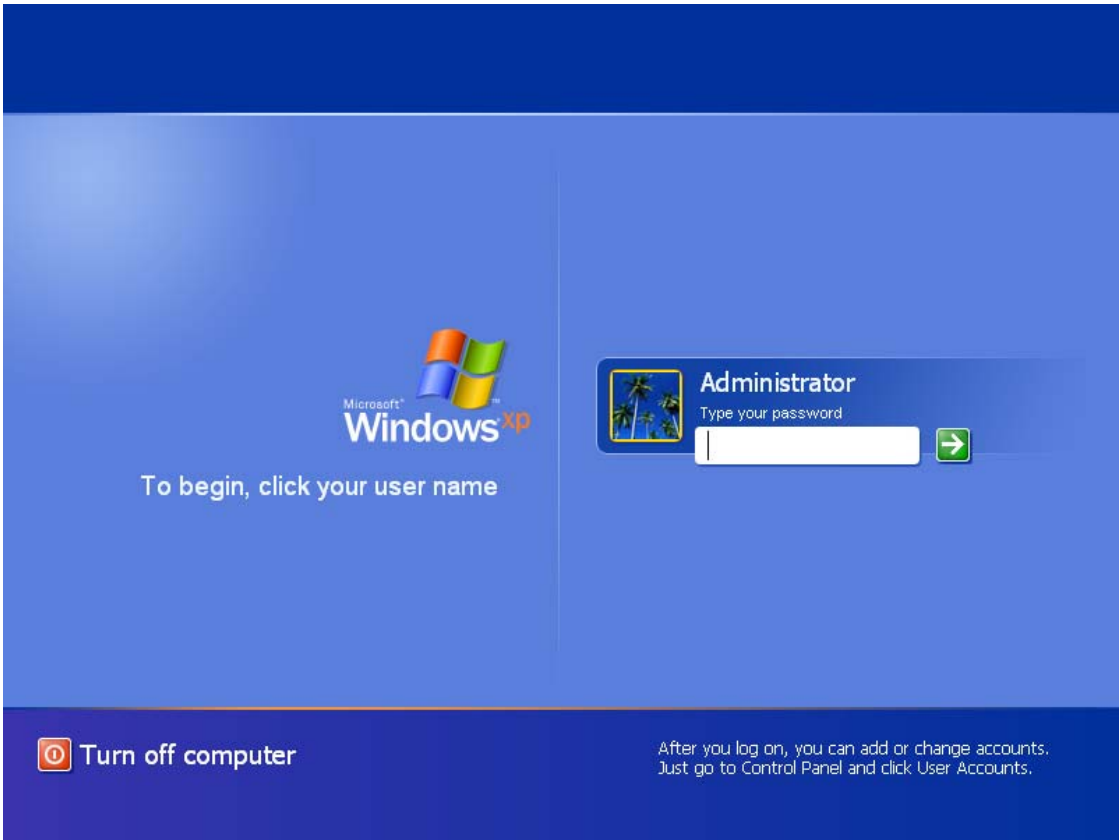
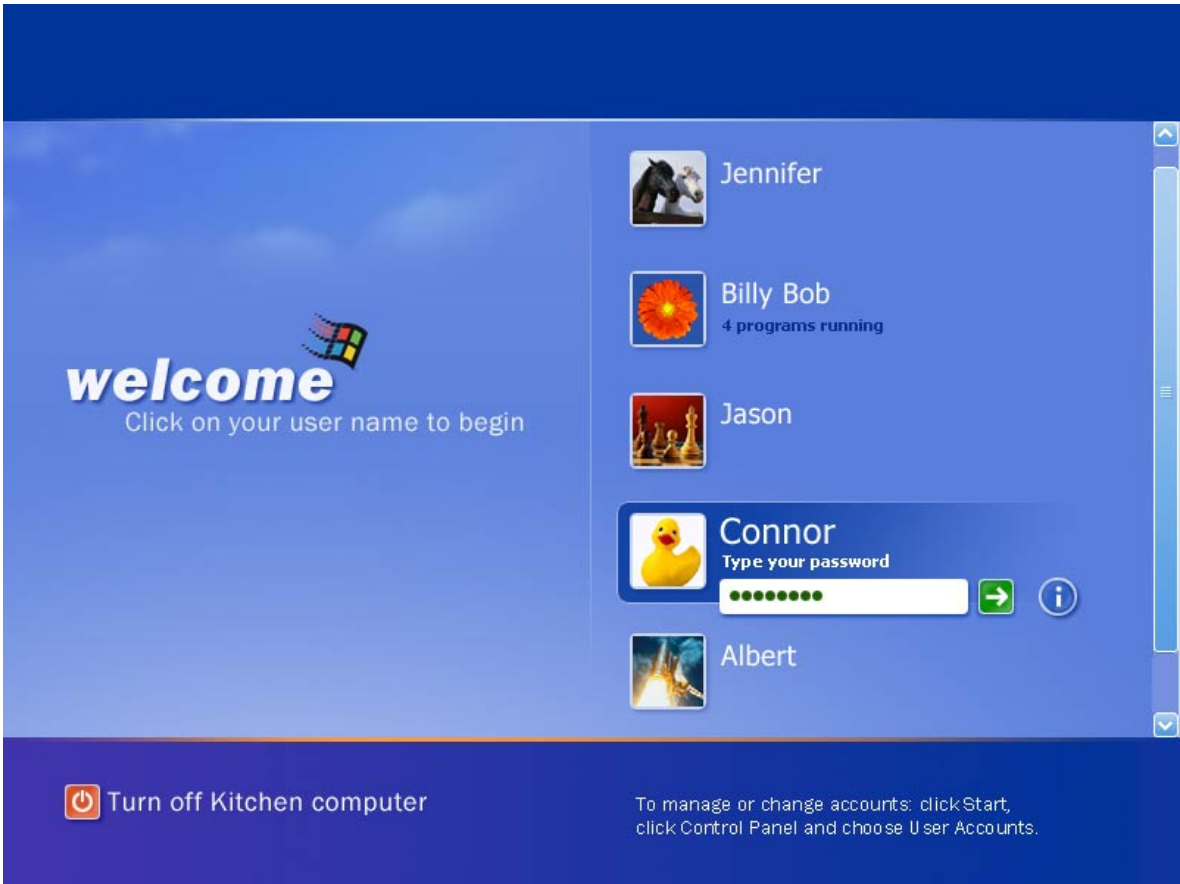


To change the picture, click on **Change the picture** and a list of pictures will appear. Make your selection and affect the change. The new picture will appear (see screen)



Remember that when you restart the computer it will come up to a Welcome screen and you need to choose which user to login. If the account is password protected, you must enter it also. All users will have settings and displays unique to the user.

Below are examples of the "login" screen, with a single user (password protected) and multiple users. (password protected)



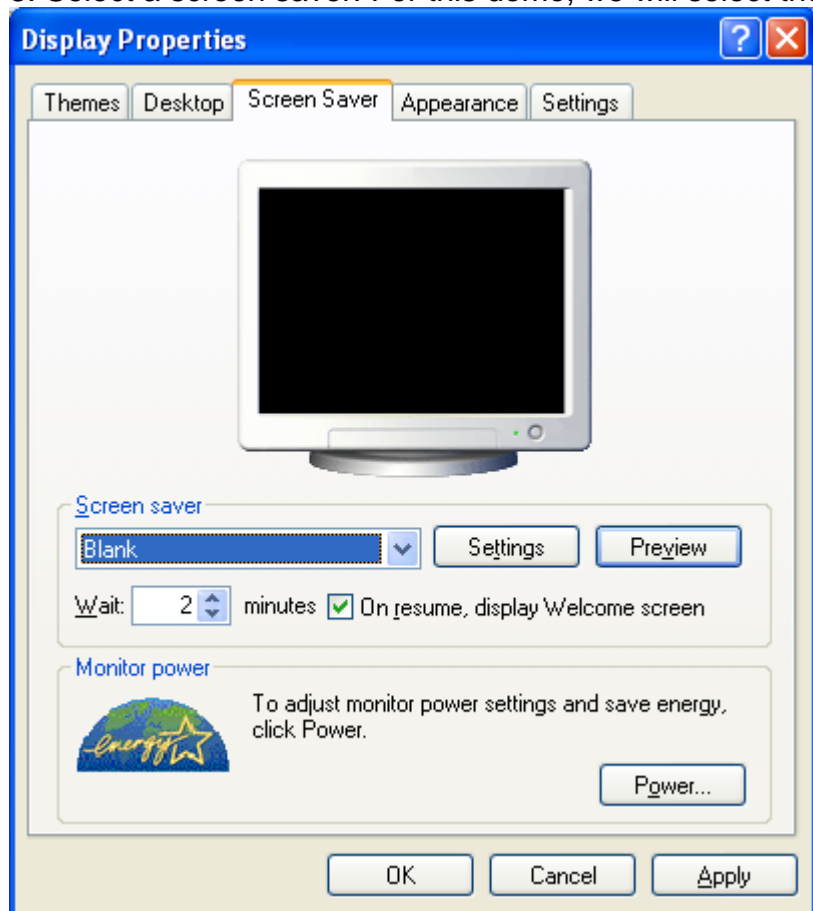
[RETURN TO TOP](#)

Windows Passwords

To create passwords in Windows, you have to have a user that has a password for his user account. From earlier we know that the user "Demo" has a password called **demo**.

To create a password so that no one has access to your computer when you have stepped away from it, you need to do the following:

1. Go to Start, then Settings, then Control Panel, and then click on Display.
2. Click on the Screen Saver tab.
3. Select a screen saver. For this demo, we will select the "blank" screen saver.



Click in the box where it says "On resume display Welcome screen".

In the Wait area, click the drop down arrow and select the amount of time when you are not present, that the screen saver comes on to protect the screen.

After the screen saver comes on, as shown above, click a key on the keyboard or move the mouse and the Welcome screen will come on. Click on your user name and enter your password and you will return to the last screen you accessed.



To begin, click your user name



Demo Account



Phillip

Type your password



 Turn off multimedia production

After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.

[RETURN TO TOP](#)

Windows Security Center

The Windows Security Center is the monitoring system for your computer. It was introduced with Windows Service Pack 2.

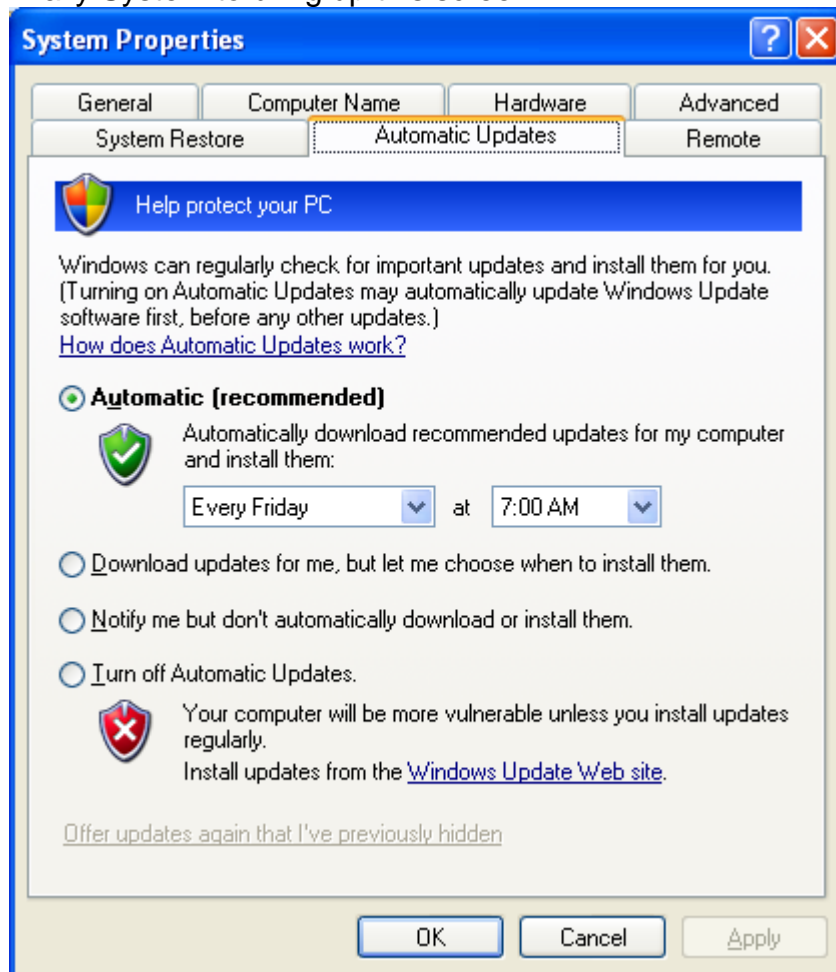
It is comprised of 3 units:

1. Windows Firewall Monitor
2. Automatic Updates Monitor
3. Anti-Virus Protection Monitor

The Windows Firewall has previously been discussed. ([Click Here for Review](#))

Automatic Updates

The Automatic Updates is accessed by clicking on Start, then Settings, then Control Panel and finally System to bring up this screen:



Click on the Automatic Updates tab.

The best setting is the one shown. However, you can choose one of the others if desired. You can, however, choose the time and day when to automatically download updates.

The updates are part of the Windows XP operating system and fix Security Issues and install tools to remove Malicious Software that is installed undetected by trips to the Internet or downloaded and installed programs.

Programs pre-installed as part of the operating system can also be updated, such as a new version of Internet Explorer or Windows Media Player. In all cases, you can choose to install or not, the safest and most secure is to allow the updates.

Anti-Virus Protection

The last item is the Anti-Virus Protection monitor. If you do not have an Anti-Virus Protection program installed, you are placing your machine in a high risk state. There are many Anti-virus programs available both free and commercially produced. Any of the following are good programs:

1. McAfee
2. Norton (Symantec)
3. Panda Software
4. Trend-Micro
5. AVG (free and purchased)

All have automatic update capability and all will protect your computer from virus problems. When your anti-virus program is not up-to-date, the marked area of the screen shown here will be in **RED**. This is the main area of the Windows Security Center. You can also turn off or choose to not have your system monitored by clicking on the down arrows here and making changes as desired.



Internet Safety & Protection

To be safe using the Internet requires some careful attention the user must exhibit. One way is not to be “duped” into false and misleading advertising or Emails.

EXAMPLES:

One item on a website might say – “you are our 1,000,000th visitor. Click here to claim your prize! Although it may look good, what you really have won is chances to have Spyware infect your machine. Spyware can best be described as a miniature program designed to track your movements on the Internet and track your equipment in-house and report back to the person/persons who designed the program.

Another equally more vicious method is through the use of Email. Often you may receive an email from a company stating that your “bank account” may have been compromised and want you to go to their website to access your account to straighten out the problem.

In truth, this is Identity Theft. No bank that has online services will EVER contact you through email if there is a problem. They must send it via the U.S. Postal Service.

Another Email method is the “attorney” or “estate manager” who wants you to help them settle an estate claim by contacting them and putting down some money to show sincerity. This is nothing more than a scam!!

Here is a good example of this scam also known as Phishing:

Recognize phishing scams and fraudulent e-mails

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

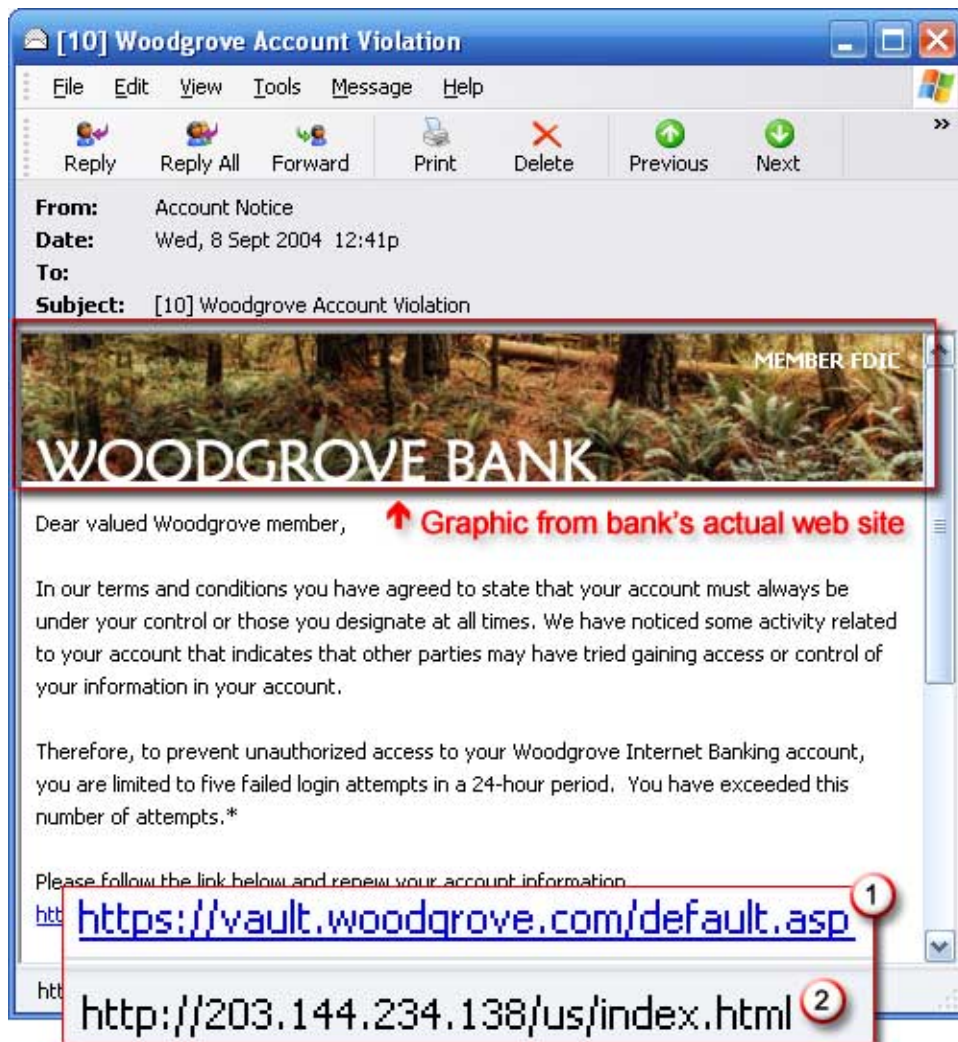
Con artists might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card company, and request that you provide personal information.

What does a phishing scam look like?

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows.

They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites.

The following is an example of what a phishing scam e-mail message might look like.



Example of a phishing e-mail message, including a deceptive URL address linking to a scam Web site

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site. These copycat sites are also called "spoofed" Web sites. Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists.

How to tell if an e-mail message is fraudulent

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

If you receive an e-mail from Microsoft asking you to update your credit card information, do not respond: this phishing scam.

"If you don't respond within 48 hours, your account will be closed."

These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishing e-mail might even claim that your response is required because your account might have been compromised.

"Dear Valued Customer."

Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site.

The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site.

Notice in the following example that resting the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.



Example of masked URL address

Con artists also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as:

www.micosoft.com

www.mircosoft.com

www.verify-microsoft.com

Use the latest products & services to protect you from online scams

Install the Microsoft Phishing Filter using [Internet Explorer 7](#) or [Windows Live Toolbar](#).

Phishing Filter helps protect you from Web fraud and the risks of personal data theft by warning or blocking you from reported phishing Web sites.

Install up-to-date antivirus and anti-spyware software. Some phishing e-mail contains malicious or unwanted software that can track your activities or simply slow your computer.

The best way to deal with Email is to use this rule of thumb: if you don't know the person or company, delete the Email immediately!!

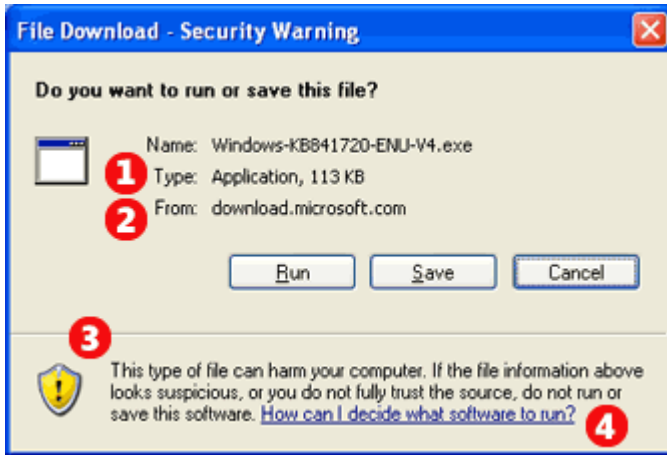
The following is good advice for being safe on the Internet...

Smart Downloading with Internet Explorer 6

Downloading files from the Internet can feel like playing a game of chance. You never know when you're going to encounter a file that damages your system. While the possibility of that happening is relatively slim, getting to know some of the security features in Internet Explorer 6 and keeping your PC protected will help you make informed decisions and avoid putting your computer at risk.

Should I Save or Open?

When you do decide to download something from the Web, you will see a box similar to the one below.



File Download dialog box

Tip: The **Always ask before opening this type of file** check box is not available for some file types, such as files with the extensions .exe or .com, which run programs or commands. When this check box is not available, you will always be asked before opening this type of file.

Save

Usually, the best option is to click **Save** to save the program or file to disk, then run or open it when you are no longer connected to the Web. This way, you can do the following before opening the file or running the program:

- Use your virus scanner to check that the file is virus-free.
- Save your work and close all your open programs.
- Disconnect from the Internet or other network connections.

For many types of files, you can ensure the most security by selecting the **Always ask before opening this type of file** check box. If you trust that a certain file type is always safe to open or run directly from the Internet, you can clear this check box.

Tip: It's easy to download software updates, games, sounds, pictures or just about anything. But sometimes it's hard to find them again on your computer. To make sure you can, create a folder where you want a downloaded file to go.

Open

Some Web sites will suggest that you click **Open** to run files from the current location when downloading. When you choose to run from the current location, the file is downloaded to a temporary location on your computer, and then you are presented with a digital certificate that gives information about the software publisher. In the certificate dialog box, you can choose whether you want to run or open the file, based on the information presented. For certain types of files this is a good option, and thanks to Internet Explorer 6 technology, you can make informed decisions about downloading this way.

What Internet Explorer 6 Does

Internet Explorer 6 verifies that a program comes from a reliable source. Though it cannot guarantee that you will never download a harmful or malicious program, it does substantially reduce the risk by checking the digital certificate that the software publisher can attach to its products.

Before you download, Internet Explorer 6 performs a check to ensure that:

- The program has a valid certificate.
- The identity of the software publisher matches the certificate.
- The certificate is still valid.

If the software has a valid certificate, Internet Explorer 6 displays certificate information, like the name of the software publisher, whether the publisher is an individual or a corporation, and the date the certificate expires. Based on these facts, you can make an informed decision about whether you want to download.

If you see a message that tells you that a piece of software does not have a valid certificate, it is also up to you to decide if you trust the publisher enough to download the software.

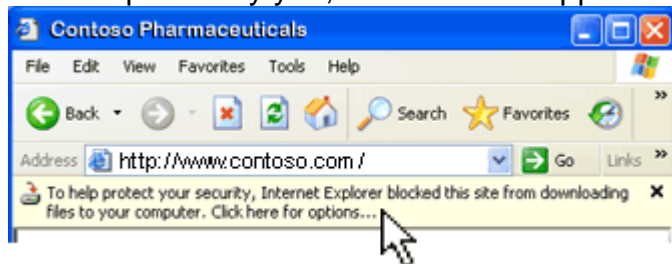
Pay attention to certificate validations, keep tabs on how your security zones are configured, and be sure you trust what you are downloading before you do it.

Improvements to Internet Explorer 6 with Windows XP SP2

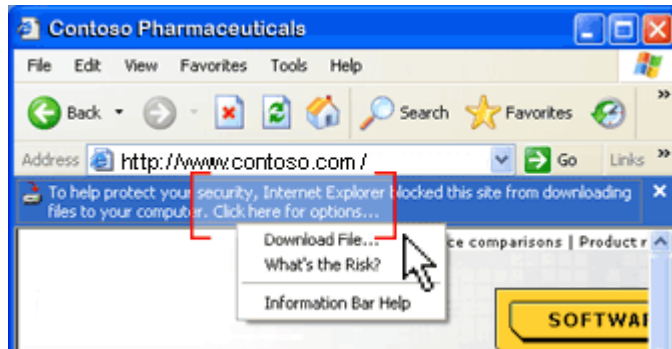
The security features and innovations in Windows XP Service Pack 2 (SP2) with Advanced Security Technologies are all about helping users like you take a proactive approach to improving the protection of your computer, your information, and your privacy. These security improvements extend to Internet Explorer 6 and downloading.

Help to Protect Your PC from Potentially Harmful Downloads

If a site attempts to download a program to your computer without your authorization, Internet Explorer 6 in Windows XP SP2 uses the Information Bar to let you know. The Information Bar shows up to notify you, and then it disappears when you move on to another Web page.



The Information Bar appears when a Web site tries to download a file that you did not request. To find out what actions you can take, simply click the Information Bar to bring up a context-sensitive menu (as shown in the following image). The menu contains a link to **Help** where you can find more information about the notification.



Click the Information Bar to see what actions you can take
Help to Protect Your PC when Saving Potentially Damaging Files

A file you download from the Web, for example, a game, a picture, or even a program can be just what you bargained for, or it can be a vehicle for more malevolent intent. For this reason, Internet Explorer 6 has stepped up its scrutiny of any file you begin to download, open, or save from the Web. Internet Explorer 6 checks to see whether the file is the type of file it says it is and provides strong warnings if there are irregularities in how the file describes itself or if there seems to be a potential for harm based on the particular type of file (as shown in the following image). Internet Explorer 6 also offers more concise information to help you understand the implications of opening or saving a file.



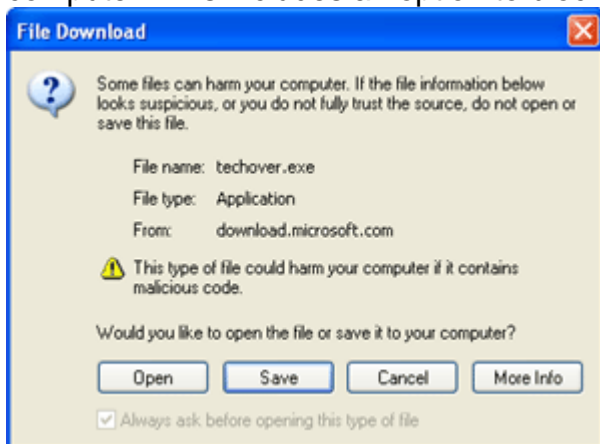
Example of an Internet Explorer 6 security warning

1. As in previous versions of Internet Explorer 6, you can see what type of file you are trying to download. In Windows XP SP2, you will also see the size of the file along with what type of file it is.
2. As in previous versions of Internet Explorer 6, you can see the source of the download in other words, where the software comes from.
3. Internet Explorer 6 also offers guidance about the type of file you are downloading.
4. You can click the **How can I decide what software to run?** Link to make a more informed decision about what to do.

Block Downloads from Specific Publishers

Some publishers will go to great lengths to have users install their programs. You may have experienced a situation in which you were repeatedly prompted to install a program that you didn't want or didn't trust. Perhaps you even installed the program just to get the prompts to go away.

Now, Internet Explorer 6 helps you to avoid this situation. With a simple click of the mouse, you have the option of automatically preventing certain programs from being installed or run on your computer. This includes an option to block all software from a specific publisher.



Now you can tell Internet Explorer 6 how to handle downloads from a specific publisher

Tip: Help keep your PC protected by downloading software updates. Microsoft Update help you keep your software current and therefore better protected against viruses and worms.

END OF TUTORIAL

[RETURN TO TOP](#)