Computer Security Basics:

How to Secure Your Windows XP Computer and Protect Yourself on the Internet

Instructors:

Ed Lee, Desktop Support Specialist
Twanda Baker, Training Coordinator
David Ladrie, Desktop Support Manager

Abstract:

This course will provide you with the tools and information necessary to properly make your Windows XP computer secure. The course will cover the use of software tools and tips you can use to keep your computer and data safe.

Table of Contents:

WELCOME!

About This Document

Desktop computer security is in the news a lot these days. With new viruses being discovered, personal information being stolen and e-mail inboxes being clogged with spam mail, it's no wonder that computer users are frustrated and concerned for their safety. Proper understanding of these threats is necessary if you're to combat them effectively.

This document was written to give you an understanding of how to secure your computer, and to help you understand why it's important to do so. It includes explanations of important concepts, step-by-step guides for many procedures, and web links to more information and downloads for helpful security programs. The information contained within is taken from the combined experience of support personnel at NC State University's Information Technology Division (ITD).

As always, the NC State Helpdesk stands ready to assist you. If you have questions about computer security or related topics, please contact our consultants:

NC State Helpdesk
919-515-HELP (4357)
help@ncsu.edu
Hours: 7:00 am – 6:00 pm, Monday – Friday

How to Read This Document

In order to make this document easy to read, you will see the following icons in several locations:

 **Key Concept**

 **Definition**

 **Helpful Hint**

These icons help to draw your attention to certain important concepts and explanations. Understanding these items will help you to effectively keep your computer safe and secure.

Explaining menus and program options can sometimes be difficult, so screenshots are also included throughout the document. By referring to these visuals you can follow along with our provided descriptions, and be sure that you are looking at the correct information.

PART ONE: SECURE YOUR COMPUTER!

Viruses and Anti-Virus Software

Viruses are malicious pieces of software, designed to spread and cause damage to programs and files on computers. Some viruses are merely annoying, displaying useless error messages. Other viruses can destroy your data and prevent your computer from working. Most of these viruses will operate transparently, so you won't even know that they're causing damage. As computer systems become more complex, virus writers have been able to craft new viruses and cause problems on a global scale. In recent years, there have been reports of companies losing millions of dollars thanks to employees being unable to do their jobs due to computer viruses. In these days of high-speed Internet connections and e-mail everywhere, everyone needs to know how to protect themselves from virus outbreaks.

Helpful Hint: NC State provides a ***free*** copy of Symantec AntiVirus Corporate Edition to all students, faculty and staff. The software may be used free-of-charge on personally owned computers, in addition to university workstations. For more information, and to download the latest version, visit **http://www.ncsu.edu/antivirus**, or see ***Appendix A***, at the end of this document.

Types of Viruses:

Because viruses do not all act in the same way, let's define the different types of viruses:

- ***Virus:*** a program that replicates and infects another program by inserting or attaching itself; basically "piggybacking" on files already present on your computer.
- ***Trojan horse:*** a program that does not replicate or copy itself, but causes damage by tricking you into opening an infected file.
- ***Worm:*** a program that makes copies of itself specifically intended to be distributed to other computers it can reach, such as via e-mail or network connections.

Key Point: All viruses are different. Some will activate at a certain date or time, but remain dormant otherwise. Others begin to attack immediately. While these different types of viruses vary in their methods, they have one thing in common: once they are on your computer, they can cause damage.

How does a virus spread?

Viruses spread through a variety of methods. The most common methods are:

- E-mail attachments
- Instant Messenger or Internet Relay Chat (IRC) file transfers and web links
- File downloads from hacked or untrustworthy web sites
- Using infected floppy disks, CD-ROMs, USB keychain drives, etc.
- Insecure computers being hacked and configured to send out viruses

This is only a partial list of methods. As virus writers become more sophisticated, they find new ways to infect computers that are connected to the Internet. The key point to consider is that anytime a computer interacts with other computers, a virus infection is a possibility.

How do I protect myself from viruses?

The most important thing you can do to protect yourself from a virus attack is to run an anti-virus program. Anti-virus software will be discussed in more detail below, but there are a few key points to keep in mind: a good anti-virus program should be relatively current and able to update itself on a regular basis, since new viruses appear all the time. Most anti-virus programs available today can automatically download and install updates, although some require you to purchase a subscription for their services. In addition, an effective anti-virus program should run at all times, so that it can catch and clean up viruses as soon as they reach your computer.

While running an anti-virus product is important, it is also important to think about what you're doing when you use your computer. There are several risky behaviors that can cause you to be more prone to virus outbreaks. Here are some easy things to remember:

Do not open unknown or unsolicited e-mail attachments.
Unsolicited e-mail attachments sometimes contain pictures, Microsoft Word or Excel documents, or other similar files. These files may actually be Trojan horses or worms that intend to spread themselves to others. If you do not know the source of the e-mail, and you were not expecting it, you should not open the attachment. Even if a message appears to come from a friend, it may not be safe. Many newer e-mail viruses will automatically send themselves out to addresses found in an infected computer's address book.

Do not download files from websites you do not recognize or trust.
While most websites that you'll likely visit are well known and trustworthy, files that get downloaded on to your computer are coming from a source that is outside of your control. If you do not know the source of a file, or you did not request to download the file, ***do not open it***. For other files that you download, use your anti-virus scanner to verify that the file is safe and not infected with a virus.

Do not use file-sharing software such as LimeWire, Kazaa, eMule or BearShare.
File-sharing programs are notorious for their use to illegally trade copyrighted music, movies and computer programs. They also spread viruses through the files they download, since the documents being traded can themselves be viruses or infected with viruses. As was described with unknown websites, if you don't know or trust the source, then you should be suspicious of the file you're receiving. In addition, many file-sharing programs come packaged with programs that show advertisements and monitor the use of your computer, which can also leave you more susceptible to virus outbreaks.

What is an anti-virus program?

An anti-virus program is designed to protect your computer from virus infections. Anti-virus products seek out viruses by comparing your files against a database of known viral threats, and will identify files that are suspicious or actual viruses. The program will then helps you determine how best to deal with these threats, including trying to repair an infected file, or deleting it in a safe manner. Every

anti-virus product will look and feel differently, so it is extremely important to become familiar with the operation of the program you choose to install on your own computer.

Key Point: You should not assume that simply installing an anti-virus product makes your computer safe. You must learn to interact with the program and understand how it operates in order to be safe.

The most effective anti-virus products have several points in common. You should insure that any product you decide to use includes these features:

- ***Regular updates:*** The anti-virus program should update itself frequently, to insure that it effectively deals with new virus threats.
- ***Background operation:*** The product should run in the background at all times, in the system tray (near your clock on the taskbar), catching viruses as soon as they appear.
- ***Virus clean-up help:*** The program should guide you through removing viruses.

The ability for an anti-virus program to update itself regularly is extremely important. As new viruses appear on the Internet, anti-virus software companies will release "virus definitions." Definitions help your program to understand how to detect new viruses.

Definition: ***virus definitions*** – files that contain information about new viruses. Virus definitions are typically updated daily by anti-virus software companies, and are used to make their products able to catch and deal with new threats.

How do I keep my anti-virus definitions updated?

Modern anti-virus software programs will update themselves automatically, without the need for human interaction. Most will wait until you are connected to the Internet, or will prompt you to connect when they need to receive updates. During a typical update procedure, the program will connect to its manufacturer's servers, and locate any new virus definitions and software patches it needs.

These programs also offer you the option to manually update your anti-virus software. In most cases the update function is made easily visible in the anti-virus program's main window. However, each anti-virus company has a different way of doing things, so you should check your software's documentation for more information. If you choose to use the software provided by NC State, look through the appendices of this document for more information.

Can I use more than one anti-virus product at a time?

No, you ***should not*** use more than one anti-virus product. Because of the way that anti-virus programs work, using two or more anti-virus scanners, simultaneously, can cause serious problems. An anti-virus program must be able to examine every file on your computer, including those that you are using. When two anti-virus programs try to scan the same files, system errors often occur.

Before you attempt to install and use a new anti-virus program, you should first uninstall any other anti-virus products. To do so, look for an uninstall icon for your program in the Start menu, or use "Add or Remove Programs," located in the Control Panel window:

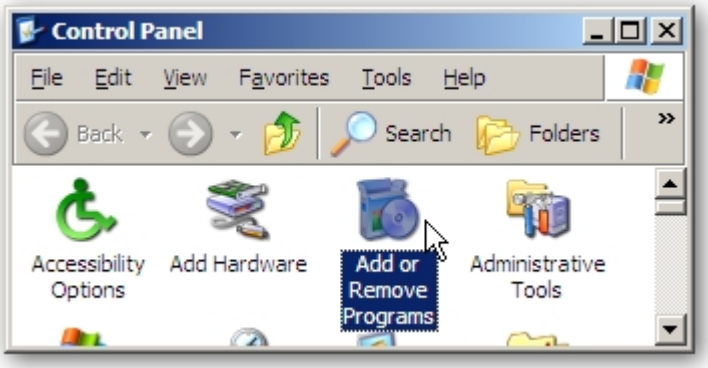


Figure 1: "Add or Remove Programs" icon in the Control Panel

Once the "Add or Remove Programs" window is displayed, locate your older anti-virus program, and click on the "Remove" button:

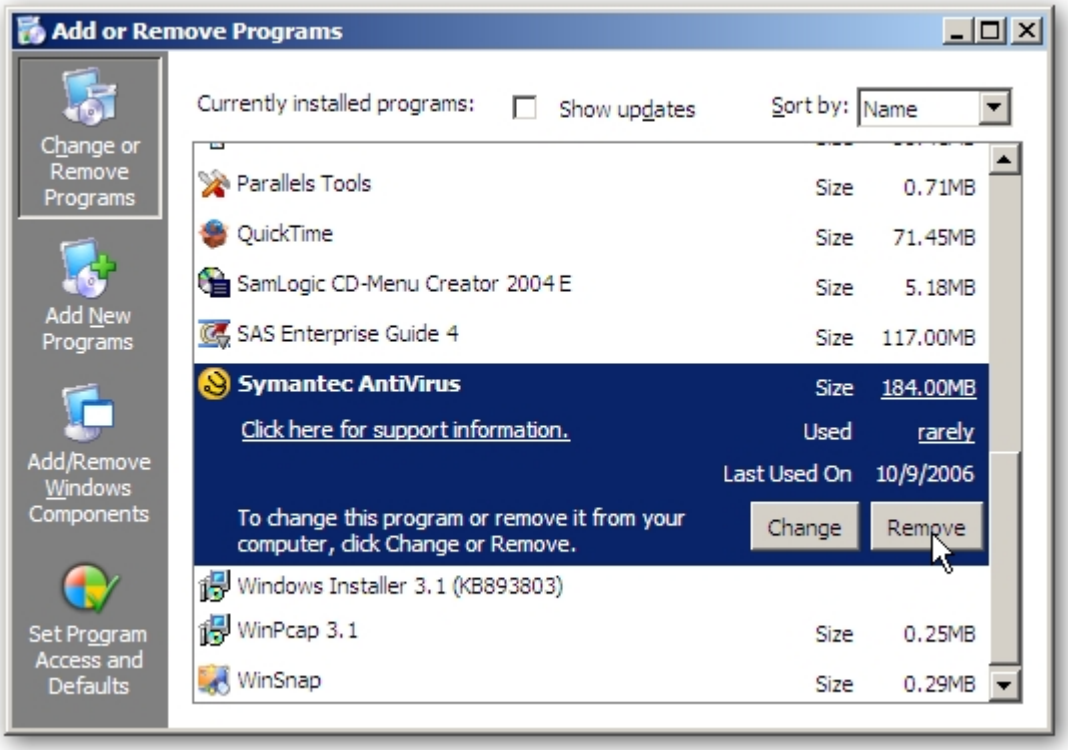


Figure 2: Removing an anti-virus program

You may have to uninstall several pieces before your older anti-virus software is completely removed. For example, Symantec AntiVirus requires that you uninstall both "Symantec AntiVirus" and "LiveUpdate." You should consult the documentation that came with your product to determine more specifically what you will need to uninstall.

Once the program is successfully uninstalled, reboot your computer ***before*** you install a newer anti-virus product. This is to insure that all pieces of the old software are gone before you continue.

When to run an anti-virus scan:

There are a number of things that should cause you to perform an anti-virus scan. A partial list:

- You notice strange behavior occurring on your computer, such as files suddenly appearing in unexpected locations (files in your "My Documents" folder, or your Desktop, that you did not place there).
- Your anti-virus program has just notified you that a virus was detected, and you wish to determine if the virus was an isolated incident or the sign of a more serious problem.
- It's your regularly scheduled time to perform a scan as a part of your normal maintenance on your computer.

Again, this is only a partial list. When you see unusual behavior on your computer, a virus scan an advisable first step to take. It can very easily help catch virus problems early on, and help prevent them from spreading and getting out of hand.

It's also important to understand that a virus scan is also a part of proper maintenance of your computer system. Much like changing the oil in your car on a regular basis, it's a good idea to run complete anti-virus scan on your computer regularly. A good rule of thumb is to perform a scan at least once every month (or more, if you use the Internet frequently). Depending on the number and size of the files on your hard drive, a full scan could take just a few minutes, or a few hours. It's best to leave the computer alone during this time, and let the scanner do its work uninterrupted.

Key Point: An anti-virus scan should be done on a regular basis, not just when you suspect that trouble is brewing. Scans performed at regular intervals will help to insure that viruses are not hidden away on your computer, waiting to immerge.

How do I run an anti-virus scan?

Every anti-virus product looks different, but they all scan your hard drive the same way: one file at a time. In order to effectively scan your computer for viruses, you should take the time to read your anti-virus product's manual. If a virus attacks your computer, you'll be thankful that you learned how to use your anti-virus program in advance.

If you're conducting an anti-virus scan as a result of unusual behavior on your computer, or after a virus was detected, is it highly advisable that you perform the scan in ***Safe Mode***. Safe Mode is a special operating mode of Windows, which allows you to perform most tasks without any virus interference. To have Windows use Safe Mode, follow these steps:

1. Turn on or restart your computer.

2. When your computer manufacturer's initial boot-up screen is displayed, begin tapping the "F8" key on your keyboard. (Note: "Windows XP" is ***not*** your manufacturer. It will be the computer manufacturer, such as Dell, HP, Gateway, etc.)

3. If you were successful, you will see a screen similar to the following:

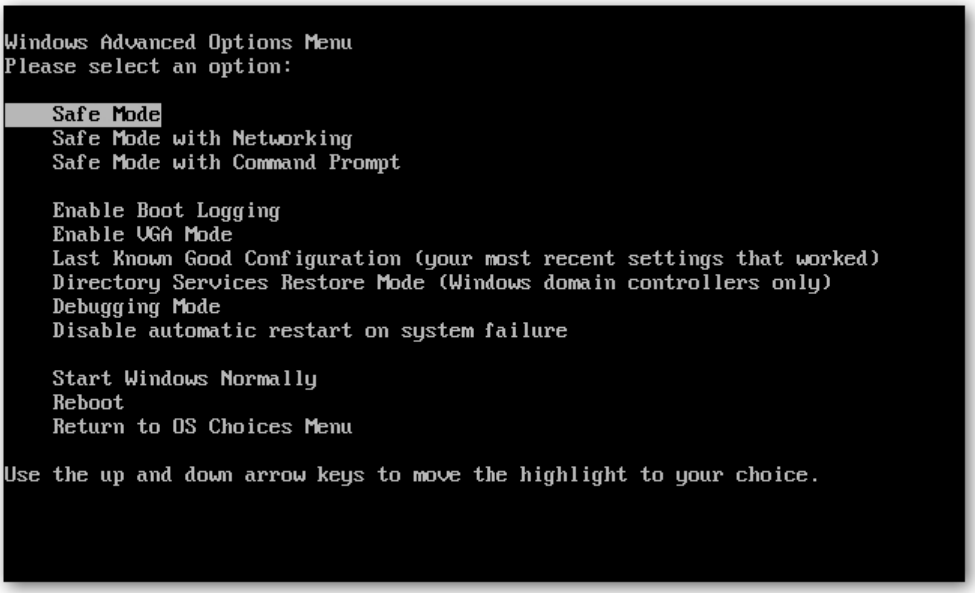


Figure 3: Selecting "Safe Mode" from the menu

4. Use the keyboard arrows to move the cursor up to "Safe Mode," then press Enter. **Do NOT** select "Safe Mode with Networking" or "Safe Mode with Command Prompt."

5. In some cases, you may be prompted to select an operating system. Again, use the keyboard arrows to choose the appropriate selection for your computer, and then press Enter.

6. In a few moments, Safe Mode will open. You may be asked to login. Do so normally, using the same user name and password that you use when accessing your computer. After a few moments, you will see a notification window similar to this:

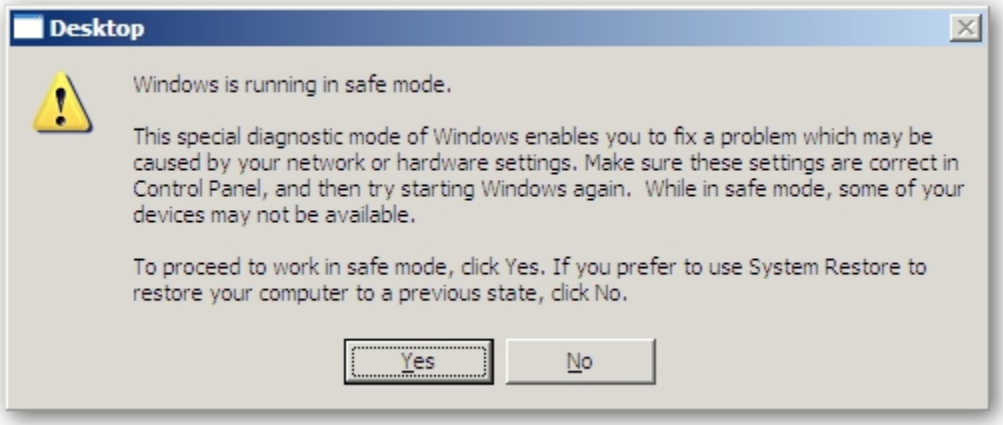


Figure 4: Welcome to Safe Mode

Once you see this notification window, you've entered Safe Mode. From here, conduct your scan normally, accessing your anti-virus program from the Start Menu.

When you scan for viruses, you should typically have your anti-virus program search through your entire hard drive. Your hard drive is usually listed as drive **C:**. If you work with files on external hard drives frequently, you should also scan them as a part of your normal virus scan.

What do I do when I have a virus?

If your anti-virus program detects a virus on your computer, it will immediately alert you to its presence, and help you clean it from your system. For example, Symantec AntiVirus will display an alert similar to this:

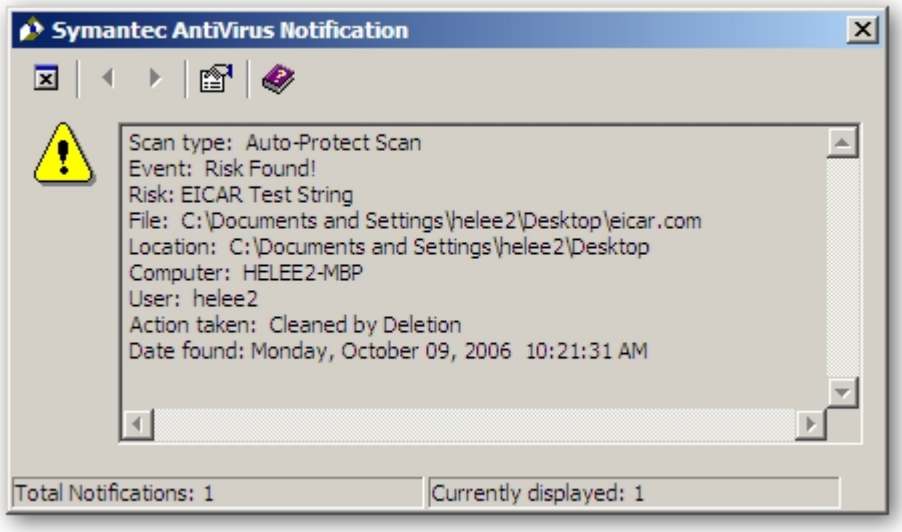


Figure 5: Symantec AntiVirus catches a virus

The notification alert window shows you the following important pieces of information:

- The name of the virus (shown in Figure 5 as the *Risk* line),
- The location of the virus,
- Any action(s) that the program took to protect your computer.

Some anti-virus programs will not take any immediate action, but rather simply recommend how you should respond to a virus threat. In any case, you should immediately make a decision, in order to minimize any damage that the virus may cause. There are typically three actions that an anti-virus program can take when dealing with a virus-infected file:

- Clean the infected file,
- Quarantine the infected file,
- Or delete the infected file.

The anti-virus scanner will either take action on your behalf, or ask you what to do.

Key Point: When a virus appears on your computer, you should not wait to deal with it. A virus alert message from your anti-virus program means that a virus is on your computer ***right now***, and you should react immediately. Follow the recommendations made by your anti-virus program.

In the best-case situation, the anti-virus program will be able to clean your infected file. This will preserve your data, and simply remove the virus that may have attached itself to the file. Assuming that the virus has not damaged the file, the file's contents can be safely retrieved and used again. While this is the best possible outcome, it is also the most infrequent.

If your anti-virus scanner is able to either "quarantine" or "delete" the virus file, you're probably safe. A successful quarantine means that the virus-infected file is still on your computer's hard drive, but has been moved to a safe location, and cannot be accessed by any other programs. By doing this, the anti-virus scanner has rendered the virus harmless. It can then be safely deleted by the user, or stored for examination later by a tech support person. When working on your own personal computer, if a virus has been quarantined, you will want to go ahead and delete it immediately. If an IT department is not supporting you, there's little value in keeping a virus around on your computer. Once a file has been quarantined, there is nothing else that can be done to fix the virus-infected file, so deleting it is the final solution.

Definition: ***quarantine*** – The state where a virus is made inaccessible and unable to execute. The virus is **not yet deleted** from your computer.

The virus scanner may also decide to simply delete the virus file, thus removing it from your system. The difference between these two options is a matter of if the infected file is or is not removed from your hard drive.

One other possibility exists: your anti-virus program may not be able to cope with the virus threat it discovers. While this is a very uncommon occurrence, it means that you potentially have a very serious problem, and you will need to take more direct action to preserve your computer and data. Read the **"How to I run an anti-virus scan?"** section on page 7 for more information on how to run a manual anti-virus scan.

Windows Firewall

Firewalls help to protect your computer from outside attack, and make your computer much safer while you're connected to the Internet. With a properly configured firewall running, your computer will be virtually invisible to the forces trying to breach your computer's security. To explain why this is important, let's first talk about what a firewall does while it's running.

Definition: ***firewall*** – A program or device that blocks un-requested communications from the Internet, preventing your computer from responding to potentially malicious attempts to gain access.

In its most basic form, a firewall places an electronic barrier between you and the Internet. This barrier examines the communications traffic going between your computer and the network. It looks to see if the traffic is something you were expecting to receive (or should see anyway). A firewall works by examining the details of "packets" of Internet traffic. If the packet appears to be safe, the firewall will allow you to receive the information. If it's not safe, or if it is ***not*** something you requested, the firewall will block the packet, and you may receive a notification.

There are two types of firewalls:

- ***Software firewall:*** a program that runs only on your computer. A software firewall is built-in to your computer's operating system (Windows XP with Service Pack 2).

- ***Hardware firewall:*** a piece of equipment that is designed to operate as a firewall, or includes firewall functions (such as many commonly-used home routers).

As was indicated above, Windows XP with Service Pack 2 has a software firewall built-in. If you have not updated your computer with Service Pack 2, you should do so immediately, in order to gain access to this feature (see the **Windows Update** section). By default, the Windows Firewall is turned ***on***. This means that your computer is immediately being protected by the firewall.

When the Windows Firewall needs your attention, it will open a window like this:

Figure 6: Firewall notification

As shown in this sample alert, when the Windows Firewall thinks something needs to be done, it will give you three choices:

- ***Keep Blocking:*** do not allow the listed program to access the Internet. Use this option when you do not recognize the program, or if you do not believe it should communicate with the network. This setting will stay in effect until you manually change it (see below).

- ***Unblock:*** allow the program to access the Internet. This tells the firewall that you consider the program to be safe, and that it needs an Internet connection to function properly. This setting also stays in effect until you manually change it.

- ***Ask Me Later:*** do not allow this program to access the Internet, but don't remember this setting. This choice tells the Windows Firewall to deny access only while the program is running ***this time***. The next time the program is used, you will be asked again.

Once you make a selection, the firewall will react accordingly. As is noted with some of these choices, the selection you make will be retained until you manually change it in the firewall settings window. Not all programs will trigger a Windows Firewall alert.

In addition, you may notice that the firewall ***does not*** make a recommendation about which choice you should make. If a Windows Firewall alert window appears on your screen, you should think carefully first, and make sure that you recognize the program. If you do not recognize the program requesting Internet access, you should probably block it.

Key Point: A firewall reacts to programs based upon the choices you make. It will not assume anything about a program or network service until you indicate how to proceed. You should be aware of the programs you're running, and not automatically accept every "unblock" request that you see.

How to I turn on my Windows Firewall?

The Windows Firewall settings are accessed through the Control Panel:

Figure 7: Windows Firewall in the Control Panel

From there, the firewall settings window will open. There are several important tabs in this window, so let's address them one at a time. First, the General tab:

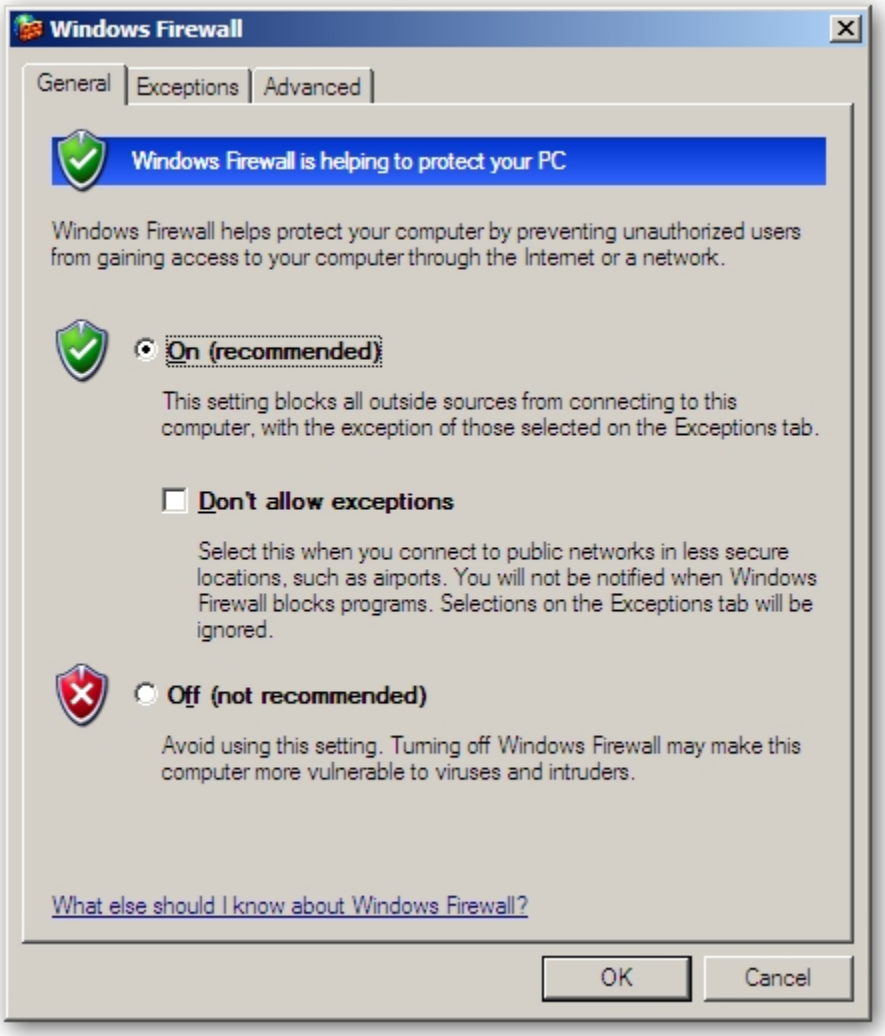


Figure 8: The Windows Firewall is turned on

The General tab gives you a simple choice: turn your Windows Firewall on or off. In order for the settings change to take effect, you must click the "OK" button.

There is also a "Don't allow exceptions" checkbox associated with the "On" setting. Selecting this checkbox will tell the firewall to ignore any "allow this program" decisions you made previously. By checking this box, you will make your firewall as secure as possible, but you might find that some programs do not work correctly. Exceptions are discussed in more detail below.

In some cases, other firewall programs may turn off the Windows Firewall. If you install a firewall program like ZoneAlarm or a security suite like Norton Internet Security, the Windows Firewall will be turned off for you. In most of these cases, it's fine to let the other program regulate this setting.

How do I manually edit my Windows Firewall settings and exceptions?

The Windows Firewall allows you to be picky about what programs and services are and are not allowed to access the Internet. These choices are called exceptions, or firewall rules.

Definition: ***firewall exception*** – A rule that you set for your firewall, telling it how to behave with respect to a particular program, service or port on your computer. The rule will either allow or disallow traffic, based upon criteria you define.

To illustrate how an exception works, let's look at some exceptions in the Windows Firewall. To see the list of exceptions, open the Windows Firewall icon in the Control Panel (see **Figure 7**). When the Windows Firewall window opens, click on the Exceptions tab:

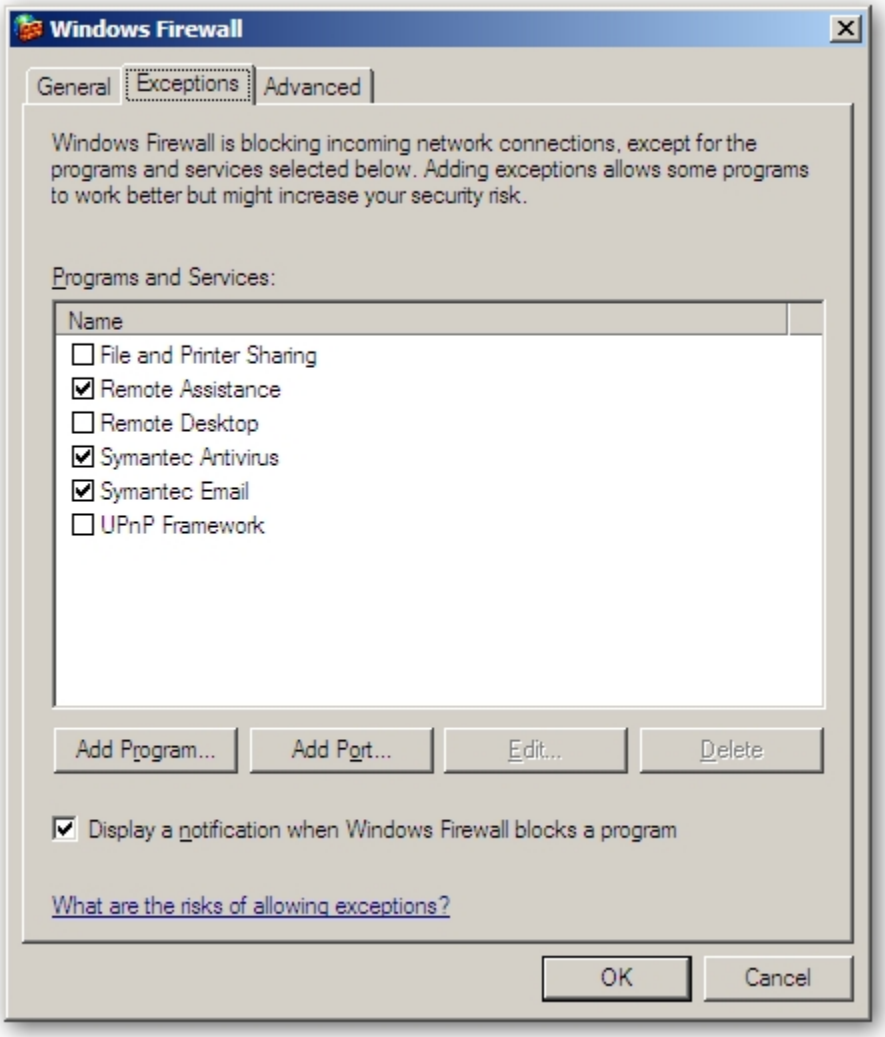


Figure 9: The exceptions list

The list in this window shows programs and services that Windows already knows about. This is typically not a complete list of Internet-using programs. This list grows over time, as more programs ask to connect to the Internet. You can also add programs to this list by clicking on the "Add Program…" button. However, since Windows will notify you when a program needs to have Internet access, you won't have to manually add programs very often. You can also use the checkbox below the list, "Display a notification…" to control if Windows will show a firewall alert message, such as **Figure 6**, when you a program requests access.

When you look at the exceptions list, Windows tries to make things easy for you. Programs with a check mark are allowed to access the Internet. Likewise, programs without a check are denied from

using the network. Your choice is meant to be a very straightforward on/off decision. Simply check or un-check the programs that you want to control. You may also use the "Edit…" button to modify the program's details, or the "Delete" button to erase it from the firewall exceptions list.

Hardware Firewalls and Home Routers/Wireless Access Points:

High-speed Internet connections have become increasingly commonplace, and sales of home network routers and wireless access points have grown. Because of the way they operate, these kinds of devices offer an extra level of security protection to the home user. A basic home router or access point can be obtained from virtually any consumer electronics retailer for under $100. The included instruction manual or CD should explain how to set up and administer the router.

Most home routers allow you to take one Internet connection (such as a cable modem or DSL) and share it amongst several computers. When you use a router, it appears to the outside world that you are using only one computer. The router determines which computer in your house should receive each piece of network traffic, and sends it out accordingly. Most routers use Network Address Translation (NAT) to determine which computer receives traffic. NAT running on a home router can protect your computer from many types of network attacks, such as port scanning and worm viruses.

Since every home router has a slightly different administrative interface, you should consult your router's documentation for more information.

Microsoft Update

Keeping modern computer software up to date is an incredibly complex process, requiring the continuous efforts of tens of thousands of programmers. Because of this constant evolution, bugs and programming errors sometimes occur. These bugs can manifest themselves in a number of ways, including causing your programs to crash or leaving your computer vulnerable to hacking. Software companies understand that in order to protect their customers, they must provide updates to their products. By applying these updates to your computer, you can insure that you do not experience problems in the future.

Definition: ***software patches/updates*** – An update for an installed application or operating system, intended to correct security vulnerabilities or software bugs. Installing these updates helps to keep your software safe and secure.

If you are a Microsoft Windows user, the most important software updates you can obtain come straight from Microsoft itself. Microsoft provides updates for their software on a monthly basis, usually on the second Tuesday of each month (often called "Patch Tuesday"). Because these patches typically repair defects in the original software, Microsoft ***does not*** charge customers for them. This means you can download them freely at any time, and continue to keep your computer protected. Free software patches are an incredible bargain for any owner of Microsoft products.

Many computer users do not realize that keeping your Microsoft software up to date is an essential part of maintaining your computer's security. Because of the overwhelming popularity of Microsoft Windows and Microsoft Office, software hackers (and even computer security experts) devote a lot of their time and attention on uncovering flaws in Microsoft's products. Because the ulterior motives of these groups differ greatly, keeping your computer's software patched regularly is a smart way to be sure that you won't be affected.

Microsoft offers two ways to keep Microsoft Windows and Microsoft Office updated:

- Automatic Updates – A software program runs on your computer periodically, checking with Microsoft's servers to find out if any software patches have been released. It will determine if any new patches are applicable to your computer, and then downloads them for you to install.

- Microsoft Update – Available via web browser at **http://update.microsoft.com**, this website lets you check in with Microsoft's servers at your convenience, and determine if there are any software patches that you should download and install.

Either of these update methods are acceptable, but we ***strongly*** recommend that you make use of Automatic Updates. By doing this, you will not have to remember to check for software patches monthly. It will do the work for you, and let you know when it's time to install.

If you have Windows XP with Service Pack 2, the Automatic Update software is already loaded on your computer. All you need to do is verify that it is turned on, and is set to connect to Microsoft regularly and download fresh updates. Thankfully, this is a very easy process. To make sure that Automatic Update is set up correctly, first open the Control Panel and locate the "Automatic Updates" icon. Double-click it to open the Automatic Updates window.

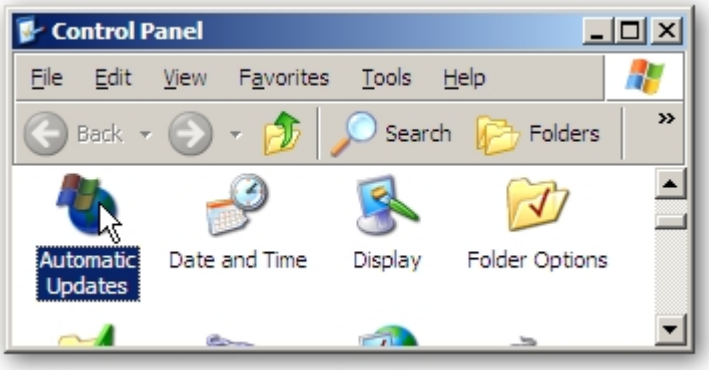


Figure 10: Automatic Updates icon in the Control Panel

In the Automatic Updates window, you will see four choices:

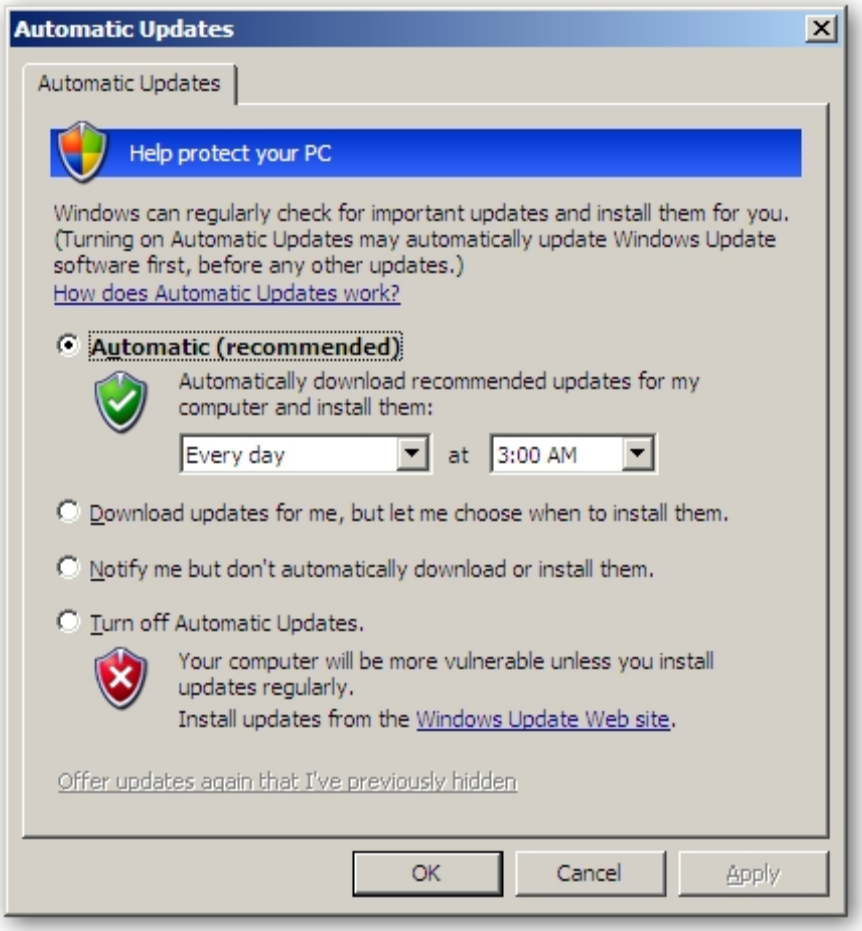


Figure 11: Automatic Updates window

These choices have the following effects:

- **Automatic (recommended):** Automatic Updates will regularly check with Microsoft, and download any applicable patches for your software as necessary. It will do this without any action on your part. Once the updates are downloaded, it will automatically install them and reboot your computer using the schedule you set. You can have Automatic Updates reboot at a

certain time on any day where it receives patches, or only on a certain day of the week. For example, you can have Automatic Updates install and reboot your computer on Friday at 5:00 pm. Please note that when this time arrives, and updates are ready to be installed, your computer ***will reboot***. Any open and unsaved documents could be lost.

- **Download updates for me, but let me choose when to install them:** Automatic Updates will check with Microsoft regularly, and download any necessary patches for your computer. It will hold these patches until you tell it to proceed with their installation. This means you must explicitly click on the "Install" button every time Automatic Updates notifies you that there are new software updates available. Having the patches downloaded on your computer ***does not*** mean that you are protected. The patches must be installed.

- **Notify me but don't automatically download or install them:** Automatic Updates will check with Microsoft regularly, but it ***will not*** download any updates. It will simply let you know that new updates are available. You must instruct Automatic Updates to download the patches in order to proceed. Again, it will take no other action until you click the "Install" or "Download" buttons. This means you will be prompted ***twice*** to complete the update procedure: once to download the individual updates, then a second time when the updates are ready to be installed.

- **Turn off Automatic Updates:** This will completely disable the Automatic Updates function. You will receive no update notifications, and your computer will not seek out any patches on its own. You will have to update your software manually through the Microsoft Update website (see the **Microsoft Update website** section below). ***We strongly recommend against turning off Automatic Updates***, because this choice will leave your computer increasingly vulnerable to attacks from the Internet. Don't take the chance.

"Automatic (recommended)" is the best selection here. This will completely automate the update process on your computer. Automatic Updates will take over the process for you, checking for patches regularly, downloading them as necessary, and installing them on schedule. This means that your Microsoft software will be up to date and as secure as possible.

Key Point: Automation of your software updating is a very smart approach to keeping your computer safe and secure. By ignoring software patches, you run the risk of your computer being easily hacked by outsiders. Don't let it happen. Let Automatic Updates do the update work for you.

If you are uncomfortable with updates being automatically installed without your approval, **"Download updates for me…"** is also acceptable. As long as you are aware that you will have to approve the installation of patches, this choice offers a balance between automation and user control.

Once you have made a selection on this window, click the "OK" button. The next time your are connected to the Internet, Automatic Updates will check in with Microsoft, and see if you need any software updates. When updates are available for your computer, you will see the following yellow shield icon appear in your system tray (next to the clock):

Figure 12: Automatic Updates icon

Please note that this yellow shield has a black exclamation mark in the middle, to distinguish it from similar icons (such as the Symantec AntiVirus tilted yellow shield).

When you click on the Automatic Updates yellow shield icon, a window similar to this will appear:

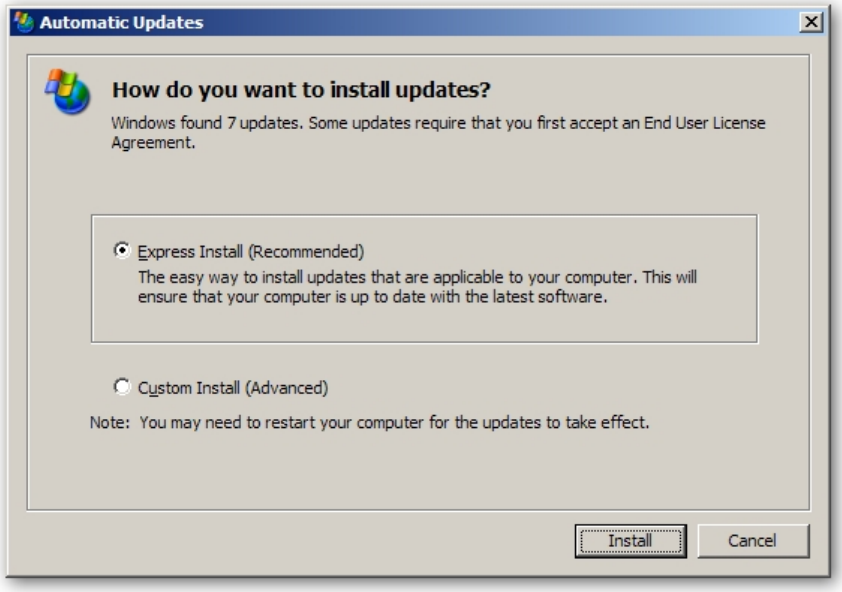


Figure 13: Updates are ready to install

You may click on the "Install" button, or choose **"Custom Install (Advanced)"** choice to see what updates are about to be loaded:

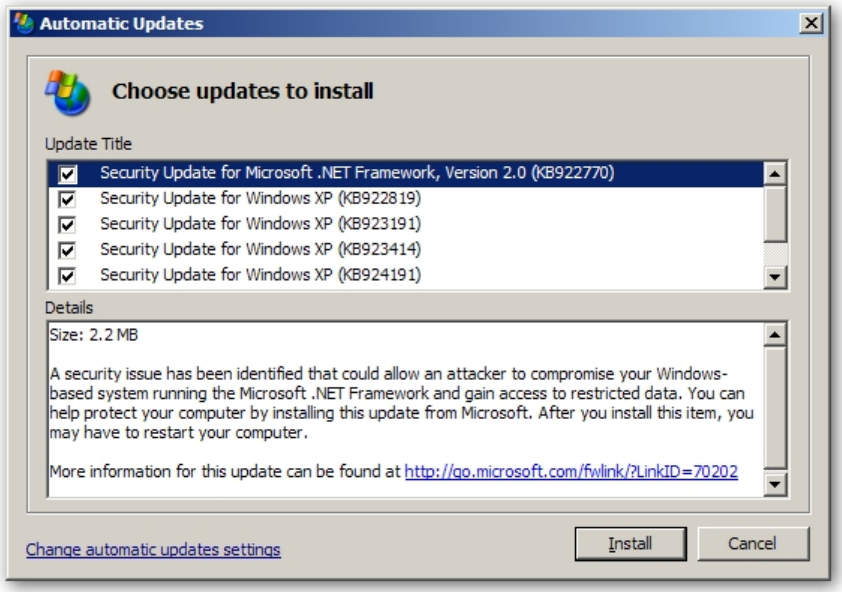


Figure 14: A listing of updates ready to be installed

You have the option of unselecting updates that you do not wish to install, by clearing the check box next to each. Unless you have a specific reason, you should not deselect individual updates. Once you have viewed the list, click on the "Install" button to proceed. In some cases, you may also be

prompted to accept an End User License Agreement (EULA) from Microsoft. Click the "I Accept" button if you wish to have the software installed.

Once the installation has begun, you can watch its progress by again clicking on the Automatic Updates icon in the system tray. A progress window like this will appear:

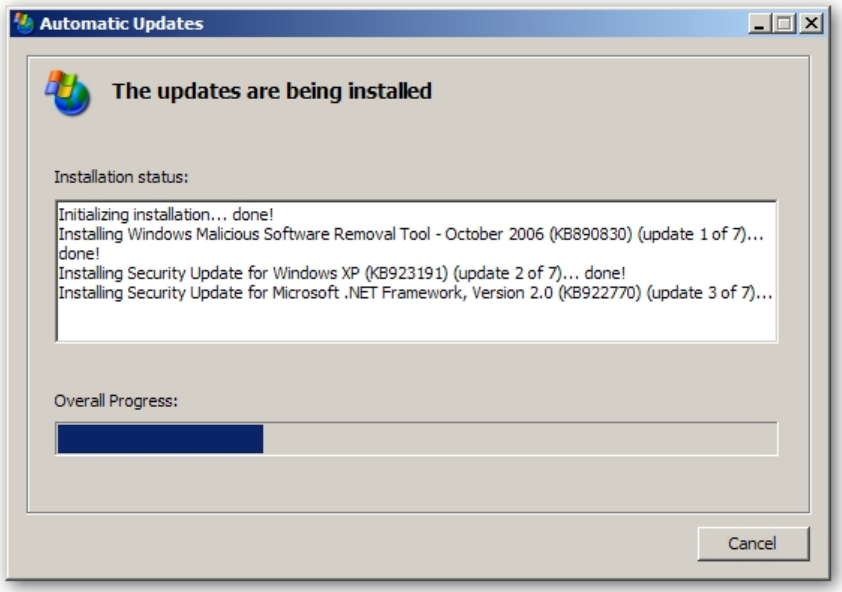


Figure 15: Updates being installed

The updates will install one at a time. When all patches have been installed, you will likely be asked to reboot your computer. If you click "Restart Now," then your computer will immediately reboot. If you click "Close," the Automatic Updates window will disappear. If you choose "Close," you will be prompted again later to reboot:

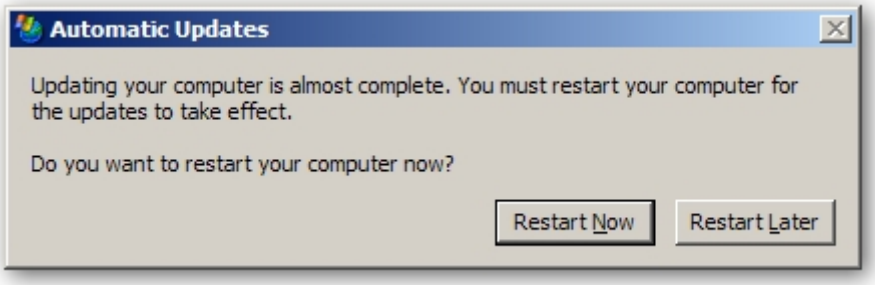


Figure 16: Reboot after updates are installed

Once the reboot is complete, your computer is up to date again.

How do I use the Microsoft Update website?

The Microsoft Update website functions as a secondary means for obtaining updates for your Microsoft software. You must use Microsoft Windows Internet Explorer. To access the Microsoft Update website, open Windows Internet Explorer and type in the following web address:

http://update.microsoft.com

The Microsoft Update website will load. You should see a webpage similar to this:

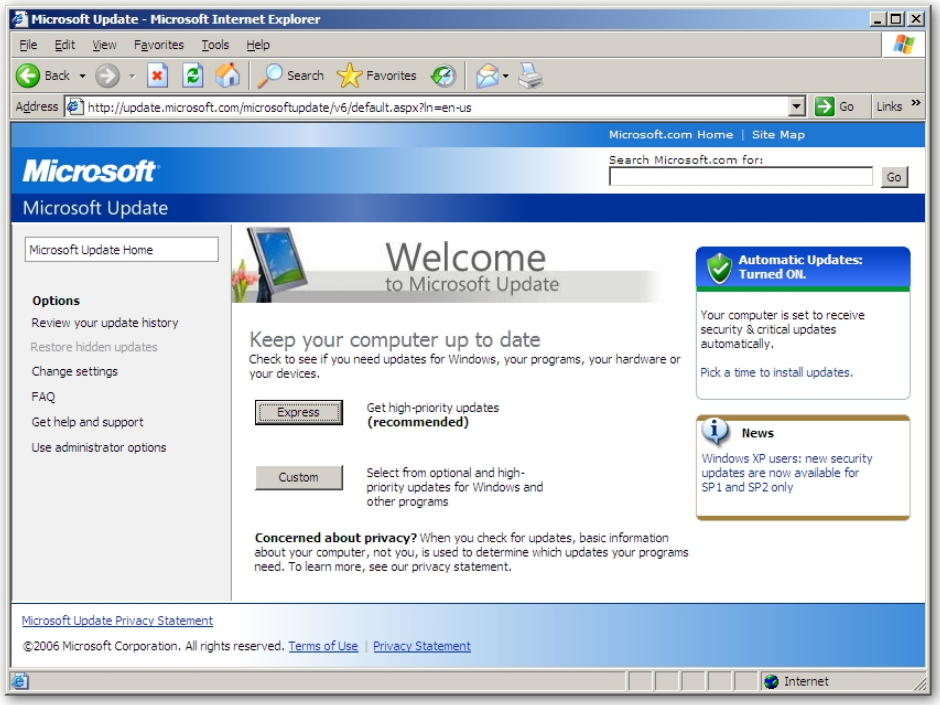


Figure 17: Microsoft Update website

If this webpage says **"Windows Update"** and not **"Microsoft Update,"** click the link above the computer monitor graphic that says **"Microsoft Update."** This will direct you to the correct location. By doing this, you will have access to updates and security patches for both Microsoft Windows and Microsoft Office.

Once you're viewing the Microsoft Update website, take note of the two buttons in the middle of the page. The "Express" and "Custom" buttons here function in exactly the same way as they do within the Automatic Updates utility:

- **Express:** This selection assumes that you want all of the current updates and begins downloading and installing them for you.

- **Custom:** This choice allows you to choose which updates to receive, similar to the Custom selection within Automatic Updates. You select or unselect individual updates, then download and install them.

On the left side of the page, you will also see several administrative choices. With these listed options, you can change your Microsoft Update preferences, get more information about the updates you've already installed (or declined to install), and even get help with how to use Microsoft Update.

From the main page, you can begin the update process by clicking on either "Express" or "Custom." Microsoft Update will scan your computer for needed software patches:

Figure 18: Scanning for needed updates

If you selected the Custom installation, you will be presented with a list of updates. You may need to use the links on the left side of the page to view all of the available patches, since Microsoft Update does not always show you optional updates. You can see lists of both High Priority and Optional updates (for both hardware and software). Microsoft Update also allows you to view the lists of updates by product instead of by type.

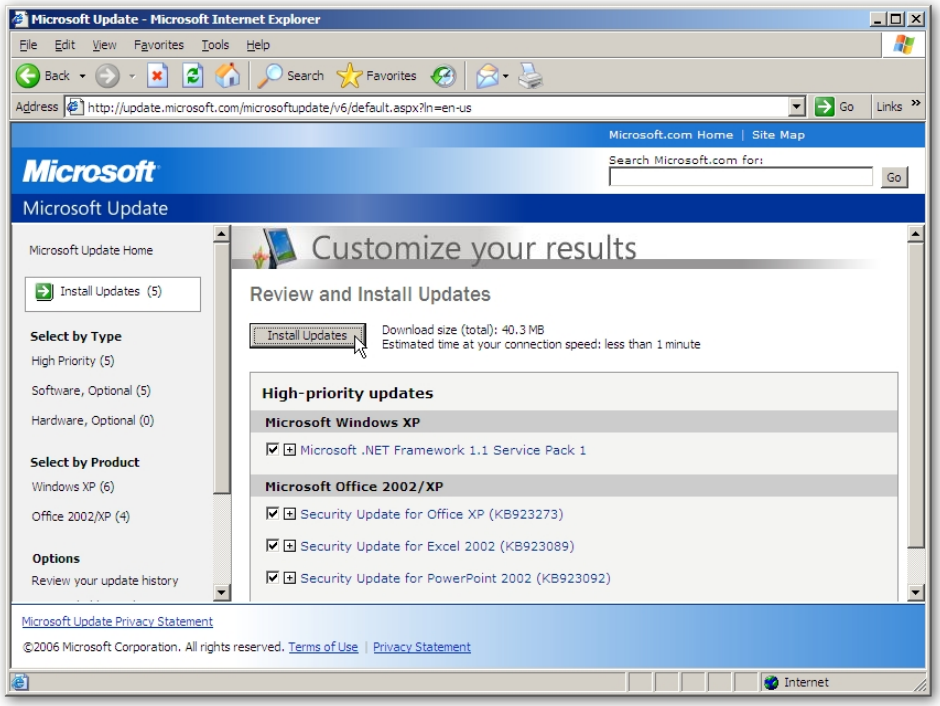


Figure 19: List of updates from Microsoft Update

Select the updates you wish to receive, and then click on "Install Updates" on the upper left. Once you review the list of updates, click on "Install Updates" and Microsoft Update will begin the process of installing software on your computer. When the update process is completed, you will be encouraged to reboot your computer. You should do so immediately.

What types of updates are available via Automatic Update or the Microsoft Update website?

Updates from Microsoft fall into one of several categories:

- **Critical updates:** patches to your software that should be immediately applied. These updates are important because they address flaws or bugs in your operating system (and other software)

that could cause your computer to crash, lose data, or be open to attacks from third parties (such as hackers, etc.).

- **Security updates:** patches that correct security flaws in Microsoft software, or enhance the security already present on your computer.

- **Recommended updates:** patches that Microsoft encourages you to download and install but are not critical to keeping your computer safe and secure.

- **Driver updates:** patches that help your computer hardware can function more effectively.

- **Other updates:** miscellaneous patches that either add new functionality to your software, or improve other aspects.

It is important to note that in most cases, Microsoft Update will offer a larger selection of patches for your software. Automatic Update will receive only Critical and Security updates.

Windows Security Center

The Windows Security Center is a feature of Windows XP that allows you to quickly check the status of your various pieces of security software. The Security Center window is a simple way to see if there are any problems, and quickly access settings as needed.

The Windows Security Center can be opened from the Control Panel:

Figure 20: Security Center icon in the Control Panel

When you open the Security Center, you will see a window similar to this:

Figure 21: Windows Security Center

The Security Center window has three major sections:

- **Status bars:** show you the current status of your firewall, updates and virus software.
- **Security settings:** lets you quickly access settings for your security programs.
- **Resources list:** find out about various security-related information.

The status bars are the most important part of the Security Center window. If each status indicator is green, then it means that Windows believes that everything is operating correctly. If any status indicator is yellow, it means that there is a problem that you need to address (such as out-of-date anti-virus definitions or an Automatic Updates setting that Windows considers insecure). If a status indicator is red, then it means that Windows believes that something is turned off or not installed. Yellow and red statuses should catch your attention and prompt you to take action. The prompts will help guide you to a solution in most cases.

Sometimes the Windows Security Center will proactively let you know that there is a problem. You may see a balloon like this appear from your system tray (near the clock):

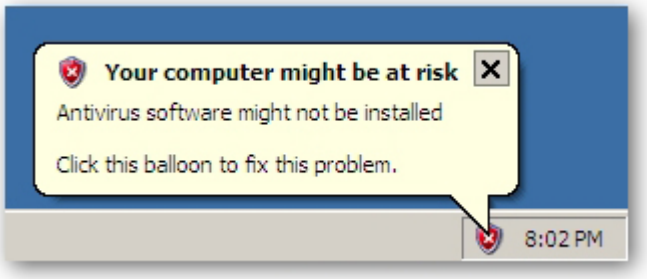


Figure 22: Security alert balloon

If you click on the balloon, you will be taken the Security Center window, where you can address the issue more directly.

PART TWO: PROTECTING YOURSELF ON THE INTERNET

Spyware and Anti-Spyware Software

Spyware and adware are an increasingly common threat, and one that is often not well understood by computer users. Spyware and adware programs, once installed on your computer, are often much harder to remove than viruses. They will often cause your computer to become sluggish, making it almost impossible to complete everyday tasks. These programs can be both a nuisance and a serious threat to your privacy and computer's security.

Definition: ***spyware*** – a program that hides itself and runs on your computer, collecting data about you. They typically collect such information as your credit card numbers, the websites you've visited, or even your passwords. This data is then transmitted to a company or individual on the Internet.

Definition: ***adware*** – a program that hides itself and runs on your computer, showing pop-up advertisements at random times, even when you're not connected to the Internet.

These programs are typically things that sound like they might be helpful in some way, such as browser toolbars, "electronic wallets," or other similar helpers. The names and descriptions are often intentionally misleading, to lull you into a false sense of safety.

In addition, some of these programs change settings on your computer. One common modification is changing your web browser's startup page (or "home page") to something different. In most cases, the new homepage will be an unknown search engine or website full of useless advertisements.

Spyware and adware programs usually end up on your computer through one of two ways:

- Spyware/adware products are sometimes "bundled" with applications downloaded from the Internet, such as P2P file-sharing programs and other free software.

- These programs sometimes get installed when you visit malicious or hacked websites using an insecure or outdated web browser.

Companies often "bundle" other software with their own products as a way to increase their revenue, not considering the implications for their users. Many of these companies do not make it easy for you to understand exactly what you're installing. They bet that you will not take the time to fully read through the License Agreement that shows on screen during the install, and will miss the "fine print." Many of these license agreements specifically state what you're about to install, including any programs that were included.

For example, the following text taken from a recent License Agreement for Kazaa P2P file-sharing software program:

> 9.1 During the process of installing Kazaa, you must install software from third party software vendors … and Sharman disclaims … responsibility for or liability related to the Third Party Software. …

> 9.4.1 Cydoor. … Sharman has partnered with Cydoor Technologies Ltd. ("Cydoor") to deliver advertisements… Cydoor's ad-serving technology is an integral part of the Software. …
>
> 9.4.2 TopSearch. … The TopSearch component regularly downloads an index of available Altnet content through your Internet connection. This index contains a list of available rights managed files which can be displayed in your search results. …
>
> 9.4.4 InstaFinder & RX Toolbar. Kazaa comes with software programs called InstaFinder and RX Toolbar … designed to redirect your URL typing errors to InstaFinder's web page … and provides you with additional website suggestions displayed as links through the Microsoft Internet Explorer window. …
>
> 9.4.6 In exchange for downloading the Software at no cost, you expressly agree that you accept the Embedded Third Party Software and that so long as you have not entirely deleted Kazaa from your computer you will not take any action… to, disable, remove, block, prevent the functioning of, or otherwise interfere with any of the Embedded Third Party Software.

The wording of the entire License Agreement is designed to force you to accept a lot of third-party software utilities, none of which have anything to do with Kazaa itself. Sharman Networks, the company that produces Kazaa, makes money by bundling these applications with Kazaa. However, they do ***nothing*** to increase the value of the program to you, the end user.

Many License Agreements for this sort of software are intentionally vague, leading an unsuspecting person to think that a third-party utility is, in fact, a part of the normal installation process. The logical question you'd wish to ask yourself is, "Do I actually need this?" If the answer is ***no***, then you shouldn't allow it to install. Make sure, during the actual installation process, that you unselect options that you don't actually need.

How can I avoid spyware and adware?

The most effective way to avoid spyware/adware is to be vigilant about what you're installing on your computer. There is no specific sort of software that is more likely to include "bundled" add-ons, so you must think carefully when you install any piece of software that you download. Thoroughly read the license agreements for programs you're installing to understand what's about to be placed on your hard drive. Carefully look over every "special offer" and "featured add-on" that comes with the product you've started to install. ***Do not*** assume that the "default" installation is the best choice.

You should also use an anti-spyware scanner on a regular basis, much the same as you would an anti-virus scanner. You should pro-actively run an anti-spyware scan at least once per month. An anti-spyware software product is designed to look for specific software threats, including many types of spyware, adware, and others, and attempt to safely remove them from your computer. To stay fully protected, make sure that your anti-spyware software is kept updated regularly.

Key Point: Spyware and adware are often harder to remove than viruses, and no any-spyware scanner is capable of removing everything. For this reason, we place strong emphasis on ***prevention*** rather than ***removal***. If you have a particularly difficult piece of spyware/adware on your computer, it may be nearly impossible to remove, even with the assistance of a technical support professional.

There are several anti-spyware software products available for free on the Internet:

- Microsoft Windows Defender
  http://www.microsoft.com/athome/security/spyware/software/default.mspx
  (See Appendix E for details on using Windows Defender.)

- Spybot – Search & Destroy
  http://www.spybot.info/en/spybotsd/index.html
  (See Appendix F for details on using Spybot – Search & Destroy.)

- Ad-Aware SE Personal Edition
  http://www.lavasoftusa.com/products/ad-aware_se_personal.php

We recommend using Windows Defender and/or Spybot - Search & Destroy, due to the fact that they offer background real-time protection, similar to an anti-virus program's background scanner. Ad-Aware offers protection only when you specifically run a scan. Windows Defender and Spybot S&D are discussed in more detail in the Appendices.

How can I get rid of spyware and adware that's on my computer?

If you suspect that spyware/adware has invaded your computer, disconnect from the Internet as soon as possible and run a complete anti-spyware scan. You should scan your entire hard drive, letting it collect as many results as possible. As the scan progresses, you will likely see multiple suspicious files when the scan is completed, and this is normal. Anti-spyware scanners typically find things that are threats to your privacy as well as outright spyware/adware software.

When the scan is complete, you should accept the suggestions made by the anti-spyware product, and let it either quarantine or delete files. In some cases, you will be asked to reboot in order to finish deleting some spyware threats. You should reboot as soon as possible.

You may find that you have better success in removing spyware and adware programs if you perform your anti-spyware scan in Safe Mode. For more information on how to open Safe Mode on your computer, see the **Viruses and Anti-Virus Software** section titled **"How do I run an anti-virus scan?"** on page 7.

E-mail Spam Filtering

A common complaint about e-mail service is the ever-increasing amount of spam messages. Spam e-mail is both a nuisance and a potential threat to your privacy, so it's smart to understand why you receive it and what you can do to get rid of it. By automating the removal of spam from your Inbox, you can spend more time reading your e-mail and less time cleaning up your account.

Definition: ***spam*** – unsolicited bulk e-mail messages, typically intended to scam Internet users out of money. Like bulk mail advertising through the postal service, these messages do not have a specific target audience, and can come from anywhere in the world.

Most spam messages are not directed at any one specific person. They are sent to thousands of e-mail addresses, in the hope that someone will decide to respond. A typical spam mail message will have a meaningless subject line, often comprised of random words. Because most of these spam mails are scams, it's usually best to ignore or delete them. Examples of some common spam messages include:

- "Generic" versions of prescription drugs
- Pornography
- Investment tips and solicitations
- Nigerian "409" treasure/inheritance scams
- Pyramid scams, including messages purportedly from big companies and wealthy investors
- Offers for discounted software (typically illegal copies)
- "Undeliverable" e-mail messages that you did not originally send

This is, of course, a partial list. In addition, many spam messages will include images and whole paragraphs of unrelated text, in an effort to defeat spam mail filters.

What is not spam?

Generally speaking, an e-mail message is **not** spam if it's something you were expecting to receive, or comes from a company with which you do business regularly (with some exceptions, see the next section on **Phishing**, page 33). A partial list of messages that are not spam:

- E-mail newsletters where you are a subscriber
- Advertisements from companies where you opt-in
- NCSU campus broadcast e-mail messages (university closings, etc.)
- NCSU crime alerts

It's important to note at this point that many legitimate companies will send you advertisements from time to time, as a part of typical promotional marketing. At the most basic level, these companies wish to keep you as a loyal customer, and they figure that if you're interested in hearing about their products, they want to keep you informed about them. When you fill out an online form (or a mail-in form) for a company's products or services, you will often be subscribed to their marketing mailing list. This is ***not*** a piece of spam, since you "opted-in" to their list. These forms often include a box you can check which says something like, "Please do not sign me up to receive advertisements."

How does a spam mail sender get your e-mail address?

Simple: it's publicly available somehow. A spam e-mail sender, commonly referred to as a "spammer," collect addresses from many locations on the Internet including public websites, e-mail groups, online web forms, and even from companies that sell your personal information. Even online message boards, such as those commonly used for online discussions, are routinely targeted. If it can be located online anywhere, then it can be potentially harvested and used by a spammer.

How can I reduce the amount of spam that I receive?

To combat spam, you have several tips and tricks at your disposal. However, it's important to point out that none of these are entirely foolproof, as spammers constantly change their approach. These techniques ***will not*** solve spam problems, but they typically make things much better.

First, use the spam filtering capability of your e-mail program. Most modern e-mail clients offer the ability to clean up spam mail coming in to your Inbox (see the Appendices for information on configuring several commonly-used e-mail clients). In addition, some Internet Service Providers (ISPs) like Road Runner and EarthLink offer spam filtering on their mail servers. NC State offers spam filtering for Unity e-mail accounts as well (see **"How can I filter spam from my NCSU Unity e-mail account?"** below).

Second, you can cut down on spam that results from these by create a "disposable" e-mail address. Using a free e-mail provider like Google Gmail, Hotmail or Yahoo! Mail, you can use this unimportant address when you fill out online forms. For example, you might not use a disposable address like "this_obviously_a_fake_address@gmail.com" on your résumé, but it would work just fine when you need to fill out a form on a website that you don't know or entirely trust.

Third, It's also important that you ***NEVER*** respond to a piece of spam mail in any way. Do not reply to it, and do not forward it. Simply delete it from your e-mail account. If you reply to a spam mail message, it's likely that the original sender will not see your response, since most senders of spam use faked "From:" addresses in their messages.

Some spam mail messages include an "unsubscribe" link. ***You should NEVER click on an "unsubscribe" link in a spam e-mail message.*** Most spammers are only interested in having their message seen by as many people as possible. When you click on that "unsubscribe" link, you're confirming that a real human actually saw the spam mail message, and that your e-mail address is a real e-mail address. That means that you've just singled yourself out to the spammer, and he/she now knows that they can send you a ***lot*** more spam messages.

How can I filter spam from my NCSU Unity e-mail account?

Your NC State Unity e-mail account can easily be configured to toss out most spam e-mail. With the PureMessage software that runs on the mail servers themselves, spam messages intended for your e-mail account can be deleted before they even reach you.

Setting up spam filtering for Unity account is quick and easy. To do so, follow these steps:

1. Open your web browser and type in the following address:

http://sysnews.ncsu.edu

2. When the ITD SysNews website loads, click on the **"login now"** link under the **"System Tools"** heading, on the right side of the page.

Figure 23: SysNews web page

3. Log in with your Unity User ID and password. When you log in, you may see one or two "secure connection" messages. Click "OK" to accept each of them, and continue.

4. Once you have successfully logged in, you will return to the SysNews webpage. Look on the right side, under the **"System Tools"** section, and click on the **"E-mail Tools"** link.

Figure 24: Selecting "E-mail Tools"

5. The E-mail Tools page will load. Look for the **"ITD Spam Filter Setup Tool"** link in the list of tools, and then click to continue.

6. The Spam Filter Setup Tool page will load. Read the page careful to understand what it will do, then click "Continue."

Figure 25: Spam Filter Setup Tool Overview

7. The tool will check to see if you have any current spam filters in place on the mail server. If it finds none, it will create and configure them for you automatically. If it finds pre-existing spam filters for your e-mail account, it will take no action.

If the Spam Filter Setup Tool creates spam filters for you, spam mail messages will be placed in a newly created **"Spam"** folder in your e-mail account. You can periodically visit the Spam folder and delete messages at your convenience. Please note that the spam mail sent to this Spam folder ***is not*** trashed for you automatically. You must open this folder and delete the messages yourself. This is done in order to give you the opportunity to review things that have been marked as spam. There is always the possibility that the filter will make a mistake, so you should occasionally check behind it.

Where can I learn more about NC State's PureMessage e-mail filters?

To learn more about PureMessage (including how-to instructions for creating your own e-mail filters), visit the following web page:

http://www.ncsu.edu/it/essentials/email_messaging/pure_message/index.html

Phishing

Phishing attacks are an increasingly common way for criminals to violate your privacy and safety. These scams target inexperienced and careless computer users, in an attempt to obtain your private information. Phishers are interested in tricking you into revealing such information as:

- Your username and password information for certain websites
- Your full name, home address, telephone number, social security number
- Your credit card information

Obviously you would not want a criminal to have access to this data, so it is important to learn the warning signs of phishing, and how to protect yourself when you're targeted.

Definition: ***phishing*** (pronounced "fishing") – unsolicited e-mail messages, warning you to update your account or security information at a particular website. These messages may have the appearance of legitimacy, but are in fact attempts to steal your private information.

Phishing scams rely upon deception and the faith of inexperienced Internet users. Phishing e-mails are specifically designed to look like legitimate notifications from various companies (including banks, online retailers, auction websites, online payment services, etc.), with the intent of fooling you into action. These e-mail messages almost always direct you to visit a similarly fake website, where you are then coaxed to divulge your personal information.

A typical phishing attack occurs like this:

1. You receive a ***seemingly*** legitimate e-mail from a company, such as eBay or a bank, indicating that your account is either being suspended or "updated" in some way, or that you've made a fraudulent purchase. You are encouraged to "click here" to log in to your account.

2. You click on the provided link in the e-mail message, and are taken to a seemingly legitimate website for the company. The website will appear authentic, and will ask you to type in your account user name and password. Even if you type in something completely wrong, you will be allowed to "log in," because no verification is taking place.

3. You will be encouraged to provide a variety of information about yourself, typically including your full name, address, and credit card number.

Your personal information is now in the hands of a criminal, who will almost certainly use it to make fraudulent purchases or even use it to obtain additional credit under your name. The sad truth is that this scenario isn't a hypothetical situation. Phishing attacks are becoming increasingly sophisticated and harder to detect, even for the most technically savvy people. However, you can reduce this threat to your privacy by knowing the signs of a phishing attack, and using an up to date web browser.

How can I avoid a phishing scam?

The best way to protect against phishing attacks is to use the latest version of your preferred web browser. Microsoft's Windows Internet Explorer 7 and Mozilla Firefox 2 both incorporate a phishing

filter mechanism, comparing websites you visit to a constantly updated list of known phishing addresses. While these filters do not catch every phishing scam, they will protect you from most.

If you visit a phishing website in Windows Internet Explorer 7, you'll see something like this:

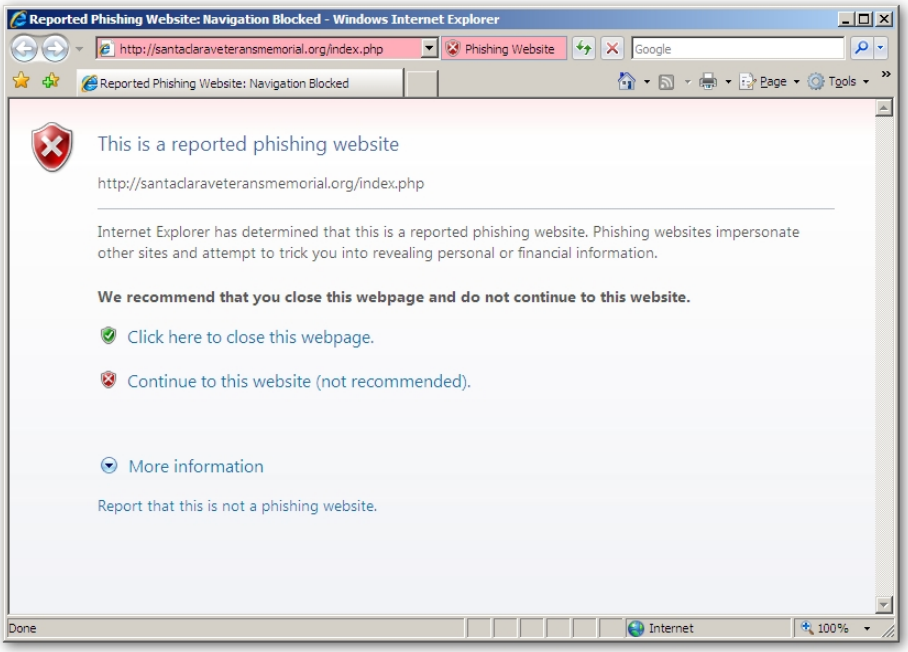


Figure 26: Phishing website notification in Windows Internet Explorer 7

In Firefox 2, you'll see something like this:

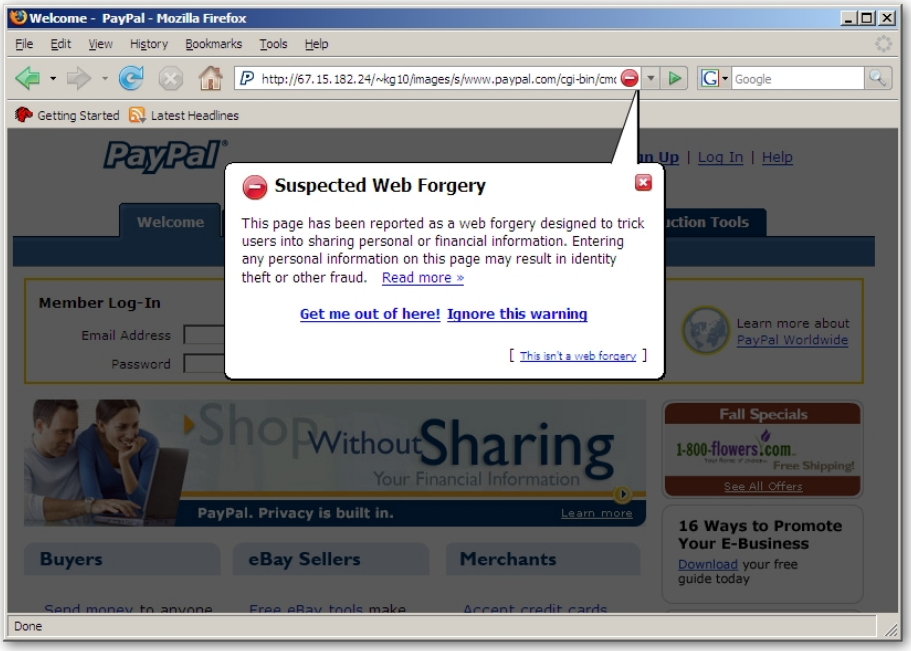


Figure 27: Firefox 2 phishing website notification

The prompts in each program will tell you how to proceed.

In addition, some web-based e-mail providers, such as Google Gmail, will notify you when a phishing e-mail is suspected:

Figure 28: Phishing e-mail notification in Gmail

You can also learn to spot some common signs of phishing. Most phishing e-mails contain logos of companies like eBay, PayPal, large banks, and other well-known companies, in an effort to look legitimate. Many of these phishing scams will encourage you to log in to a website and update your account information, suggesting that your input is "urgently" needed. These messages play upon your fears, and are sometimes intentionally worded to sound like you've done something wrong.

When you receive a seemingly legitimate message like this, you ***should not*** use the links provided in the e-mail to open the company's website. Instead, call the company via telephone, or open up your web browser and access the company's website on your own. If the phishing e-mail is asking you to urgently "update" your account information, find out from the company first if there is a specific and justifiable reason for needing the information again.

You should also insure that any time you are providing personal information about yourself that your web browser is connected to a secure website. To learn more about secure websites, see the next section, **Web Browser Security**, starting on page 37.

What can I do about Phishing e-mails?

If you've received a phishing e-mail, chances are good that others have received it as well. What's unfortunate about this is the fact that there's always someone that will be duped into providing their personal information, making the phishing attack a success. However, there's something that you can do about phishing: you can report phishing messages and websites. By doing this, you can help to protect others from falling victim to these come-ons.

Phishing e-mails: When you decide to forward on a phishing e-mail, make sure that you send the ***full headers*** along with the message itself (consult your e-mail program's help documentation for instructions on how to access this information). Some of the more important addresses where you can send copies of phishing messages:

- All phishing attempts can always be forwarded on to the Federal Trade Commission, **spam@uce.gov**.
- eBay-related phishing e-mails can be forwarded to eBay's Fraud Protection department, **spoof@ebay.com**.

- PayPal-related phishing messages can be forwarded to PayPal's Account Protection group, **spoof@paypal.com**.

If you use Google Gmail, you can also mark any message in your mail box as a phishing message. Open the message, then click on **"Show options,"** in the upper right corner of the message display. Once the options are displayed below the message headers, click on **"Report phishing:"**

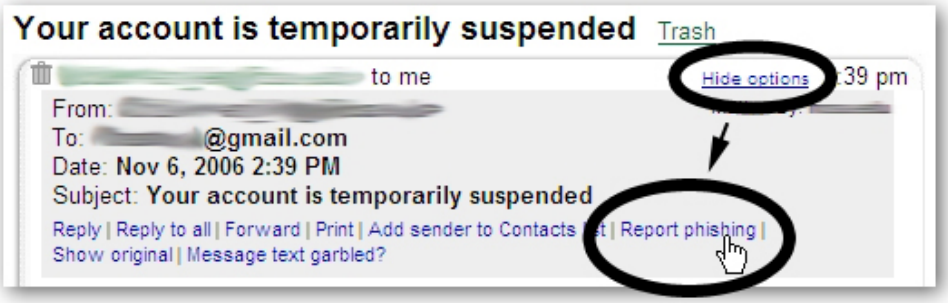


Figure 29: Reporting phishing e-mail in Gmail

Phishing websites: If you click on an e-mailed web link, and end up visiting a website that you suspect to be a phishing site, you can report it. Microsoft and Mozilla maintain constantly-growing lists of known phishing websites, which your browser can warn you about. If you use the latest versions of either Windows Internet Explorer or Mozilla Firefox, you can use their built-in reporting features to add to their phishing databases. In fact, the database used by Firefox is the same one maintained by Google for Gmail.

First, make sure that you're actually ***currently*** looking at the suspected phishing website. All of these tools require that you report the site while you're visiting it, not before or after the fact.

In Windows Internet Explorer 7, you can report a phishing website by opening the **Tools** menu, then selecting "Phishing Filter," then click on "Report This Website."

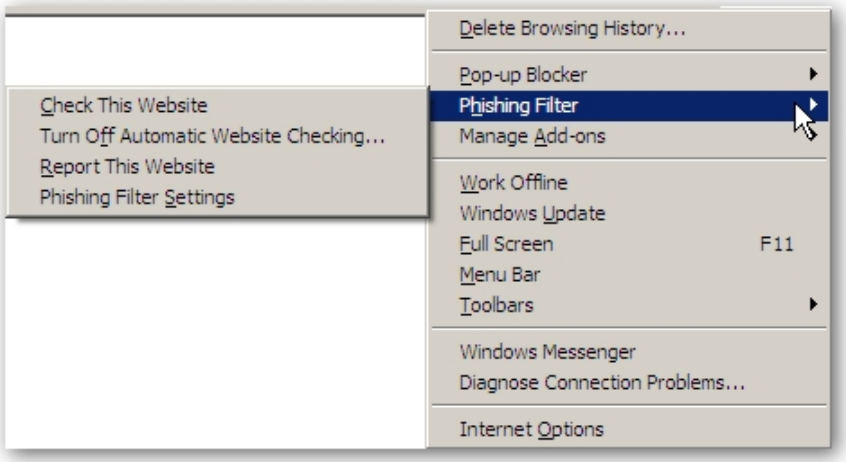


Figure 30: Opening the Phishing Filter menu in Windows Internet Explorer 7

A new window will open, asking you to confirm the details of what you're reporting. Make sure that you click the check box that says "I think this is a phishing website."

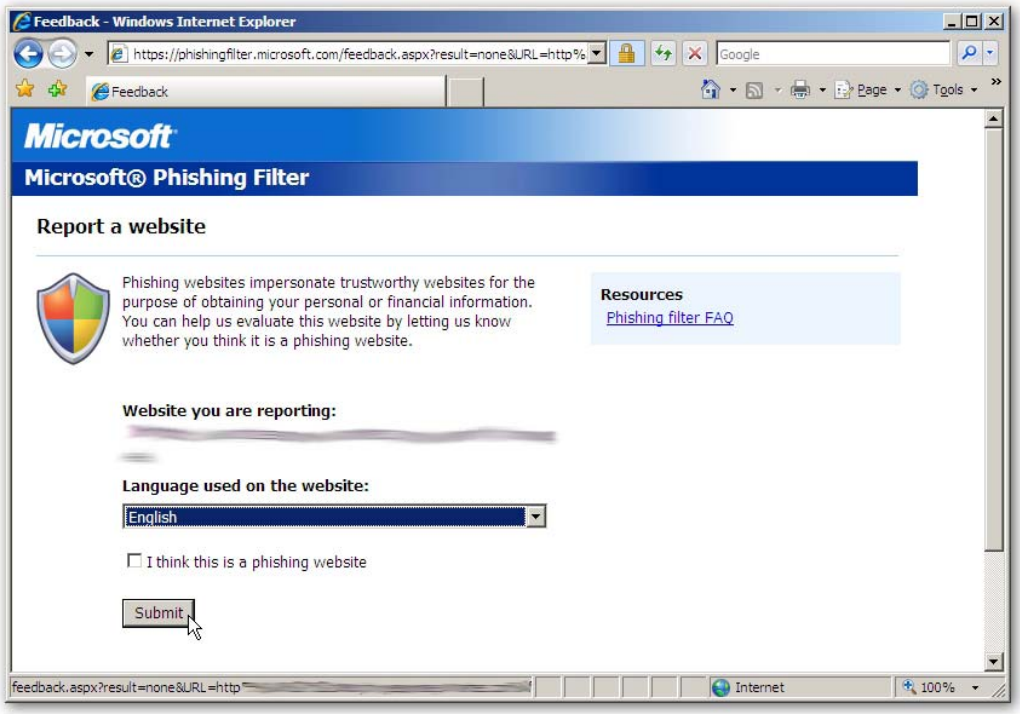


Figure 31: Reporting a phishing website in Windows Internet Explorer 7

In Firefox 2, the process is similar.

To report a phishing site, open the **Help** menu, then click on "Report Web Forgery."

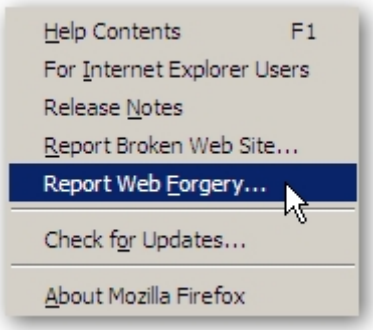


Figure 32: Reporting a phishing website in Firefox 2

You will be asked to confirm that this is a suspected phishing website. You can add additional comments if you wish, then click on "Submit Report."

In addition, you can report phishing websites to a third-party database, known as **Phishtank**, located at **www.phishtank.com**. In order to do so, you'll need to know the web address of the phishing website, which you can easily copy from the Address bar of your web browser, while you visit the phishing site.

Web Browser Security

A web browser is only as secure as the person that uses it. When you're surfing the web, there are a few things you can do to protect yourself from fraud and having your computer hacked. The items listed here are a good starting point.

Keep your web browser updated:

First, make sure that you are using an up-to-date web browser. Microsoft and Mozilla provide regular updates for their web browsers, and make it easy for you to stay current. Microsoft's Windows Internet Explorer is kept updated via Microsoft Update (see the **"Microsoft Update"** section, page 16). Firefox updates itself automatically, and pops up a dialog box when it's time to install a new version.

Check for secure server connections:

Second, when you are visiting websites where you're asked to login or provide personal information, it's a good idea to make sure that they're listed as secure websites. Secure websites encrypt your data, to prevent unauthorized people from viewing the information as it travels across the Internet between you and the server. Check the beginning of the web address in the address bar – it should be **"https://"** rather than just **"http://"**. Also check to see if there's a lock icon on the browser address bar, or at the very bottom of the browser window. It will typically look like one of these:

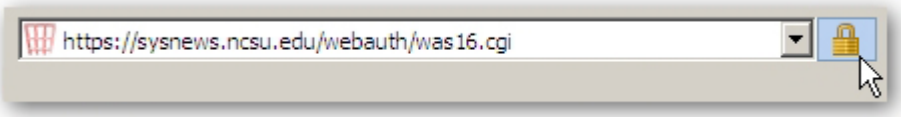


Figure 33: Secure website lock icon in Windows Internet Explorer 7

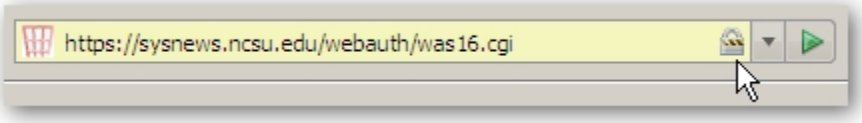


Figure 34: Firefox 2 secure website lock icon

A lock icon and an "https://" address are good indications that the website is a secure website.

When you visit some secure websites for the first time, you may be prompted to install a "security certificate." This certificate essentially serves as a "seal of approval." It indicates that an independent security company, often called a "certification authority," has verified the security of the server.

Your web browser is pre-programmed to accept security certificates from well-known companies. You typically do not see notifications about these certificates because they're considered safe. However, some organizations, including NC State University, also issue security certificates, proving that a website is considered secure and ready for use. These are often called "self-signed" security certificates. While these certificates are usually safe, your web browser will likely give you a security warning when you first encounter one.

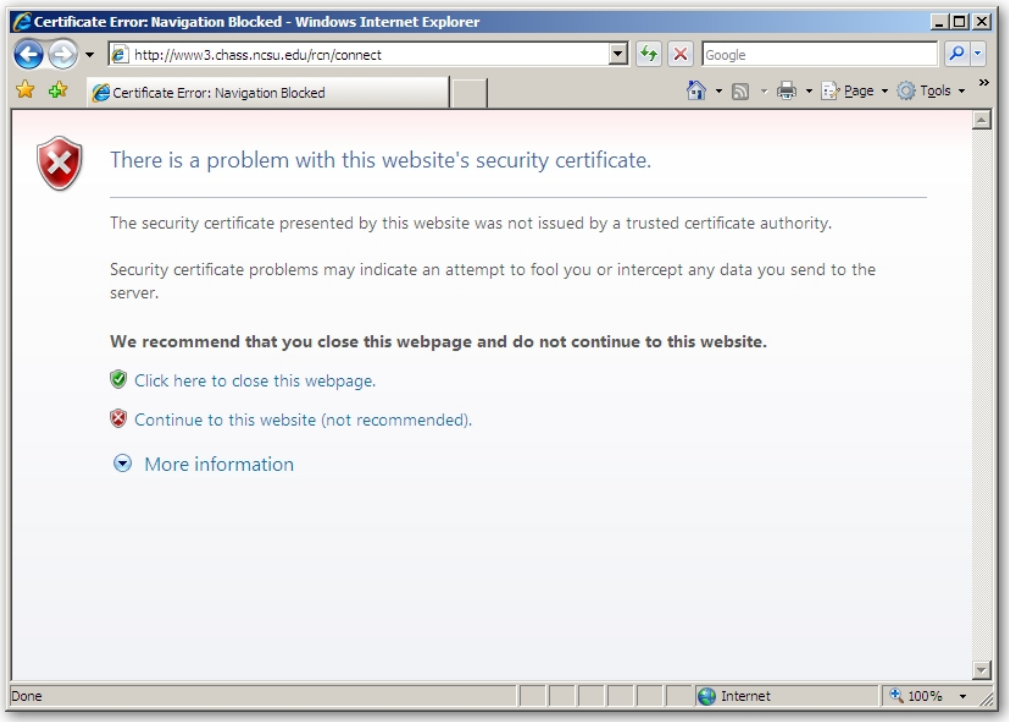


Figure 35: Security certificate alert in Windows Internet Explorer 7

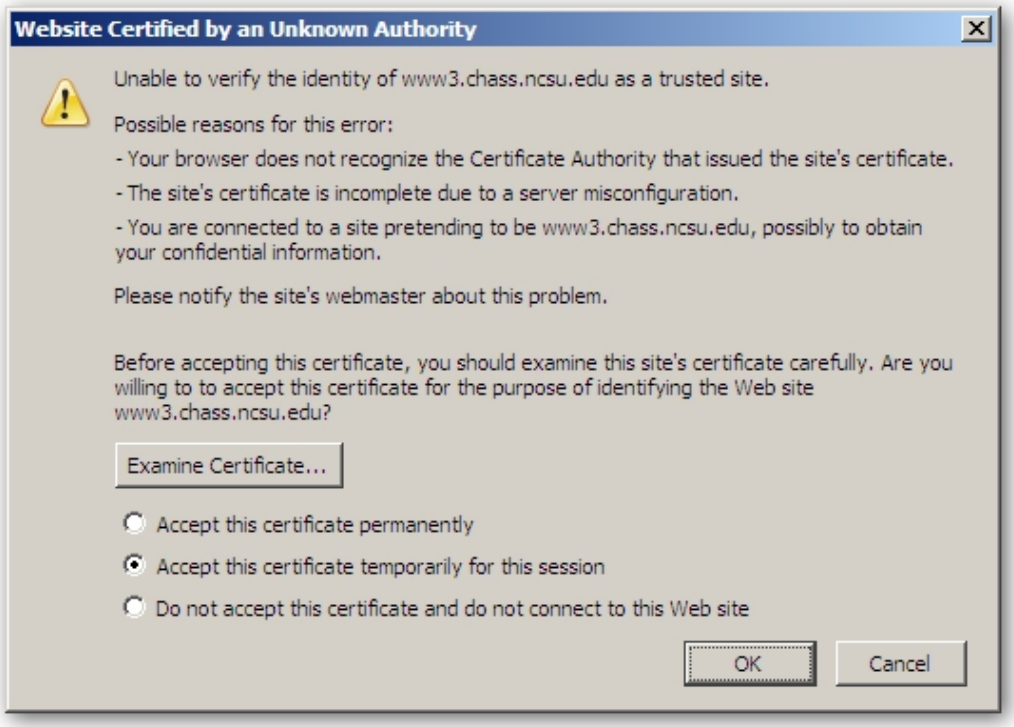


Figure 36: Security certificate alert in Firefox 2

As you can see, you will be given two or three options, depending on your web browser. These typically include: permanently accept the certificate, temporarily accept it, or reject it outright. If you think you can trust the security certificate, then click on "accept."

Key Point: Most major companies ***do not use*** self-signed security certificates. They rely upon certificates issues by outside companies. By doing this, their internal practices and security measures can be independently tested, and verified to meet necessary standards. A self-signed certificate being used by a seemingly legitimate website should be treated with skepticism.

It's important to note, however, that self-signed security certificates are not always a problem. As was mentioned before, some companies do use self-signed certificates as a way to keep your data protected. NC State University's Information Technology Division issues security certificates to show that university web servers are properly secured. While these ITD-issued certificates are not from a major company, they are useful and appropriate on an NCSU website.

An NCSU security certificate can be downloaded and installed in your web browser. By installing this certificate, you can insure that your secure connections with NC State's websites are safe. The security certificate can be found at this web address:

http://www.ncsu.edu/itd/security/ca-itd.html

Click on the download link on the page, and then open the certificate file. In Windows Internet Explorer 7, you will see a window providing details about the security certificate:

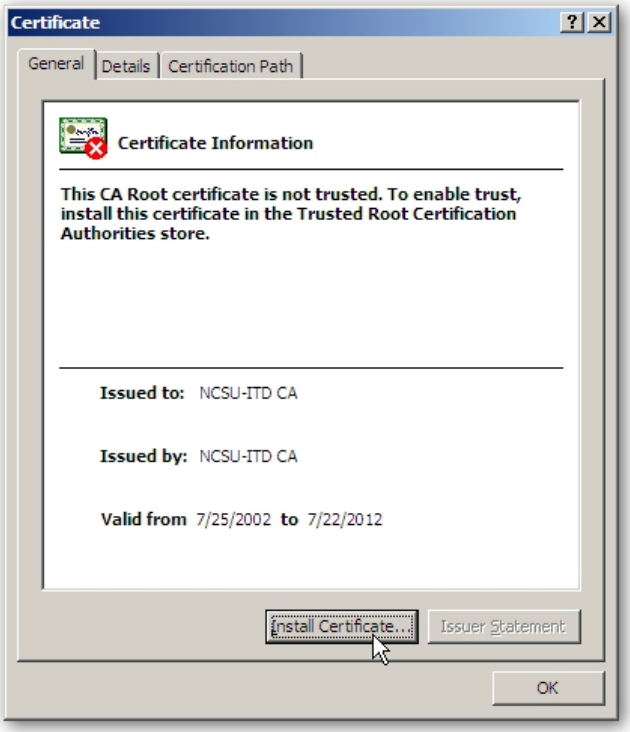


Figure 35: Security certificate in Windows Internet Explorer 7

Click on the "Install Certificate" button, and follow through the setup steps. You will not need to change any settings in order to complete the process.

In Firefox 2, the process is easier. When you click on the download link on the page, you will be presented with a window like this:

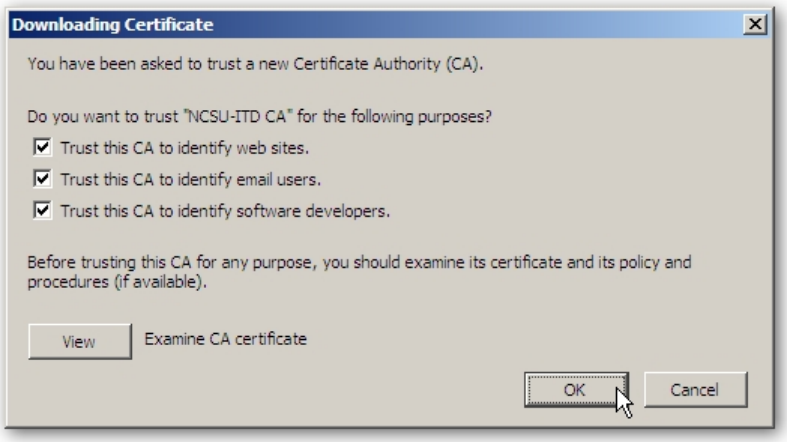


Figure 36: Installing the security certificate in Firefox 2

Make sure that all three checkboxes are checked, and then click the "OK" button. The certificate will install itself without any further steps.

Use a pop-up advertisement blocker:

Third, make sure that your browser's pop-up advertisement blocker is turned on. Pop-up ads are annoying, and can sometimes contain malicious code. You're much better off simply preventing them from even appearing on your screen.

Modern web browsers have pop-up blocking functions as a standard feature. You do not need a third-party pop-up blocker. In Windows Internet Explorer 7, the pop-up blocker can be accessed from the Tools menu. In Firefox 2, pop-up blocker settings are available in the Options dialog box, which is also found in the Tools menu.

Don't save your passwords in your web browser:

If your computer's security is somehow compromised, anything stored on it is at risk of being copied or deleted. One of the first things a hacker might look for is your account information and passwords. For example, if you have your bank account ID and password saved in your web browser, it could be accessed and copied if your computer were attacked. Imagine how much damage that could do to your finances and creditworthiness. And that's just one possible scenario.

Most modern web browsers will offer to store your password for you, ostensibly to make it more convenient to gain access to websites you often visit. While this is certainly a handy feature, it's also one that's easily exploitable by someone seeking to cause you harm.

One easy way to prevent this sort of thing from occurring is to ***not store your passwords*** in your web browser. If your web browser asks to store your password, just say "no." By doing this, your password will not be stored on your computer, meaning it can't be retrieved by someone that's gained unauthorized access to your PC.

Strong Passwords and Computer Account Security

What is a strong password?

One of the easiest ways to keep your computer safe is to use a hard-to-guess password. These "strong" passwords typically contain a combination of upper- and lower-case letters, numbers, and even some special symbols (like !@#_$%^&). Dictionary words and easily guessed numbers (like your telephone number, street address or date of birth) are not secure enough. Every password you use should be at least 6 characters long, and longer is always better. Here are a couple of examples:

- Use numbers and symbols in place of letters, and vary your capitalized letters. For example, instead of "Michael 25," try something like this: **m!cha3L_25**
- Combine a few pieces of information. For example, if your birthday is October 24th, and your dog's name is Rover, try combining the two, like this: **RoVeR&1024**
- Use a longer phrase (no spaces!). For example, from "Moby Dick:" **CaLL_m3_IshmAeL**

Your password should:

- ***Never*** be an easily-guessed word or phrase like "password" or "letmein"
- ***Never*** consist of a single word or a *simple* combination of words (such as "capitalcity")
- ***Never*** use any part your first or last name, or the names of your children or pets
- ***Never*** include your full date of birth, social security number, or other important dates

How to I change my password on my computer?

The account on your own computer should have a password. If your computer account does not have a password, someone on the Internet, or even someone that is just within physical proximity, can freely access it. This is one of the most commonly exploited security vulnerabilities, and it's easy to correct.

To add or change your password specifically on your computer, follow these steps:

1. Open your Control Panel, and open the "User Accounts" icon.

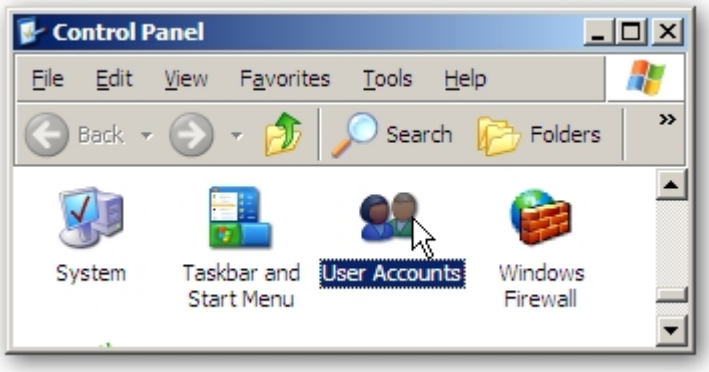


Figure 37: User Accounts icon in the Control Panel

2. Look for your account name in the list on the bottom, and then click on it.

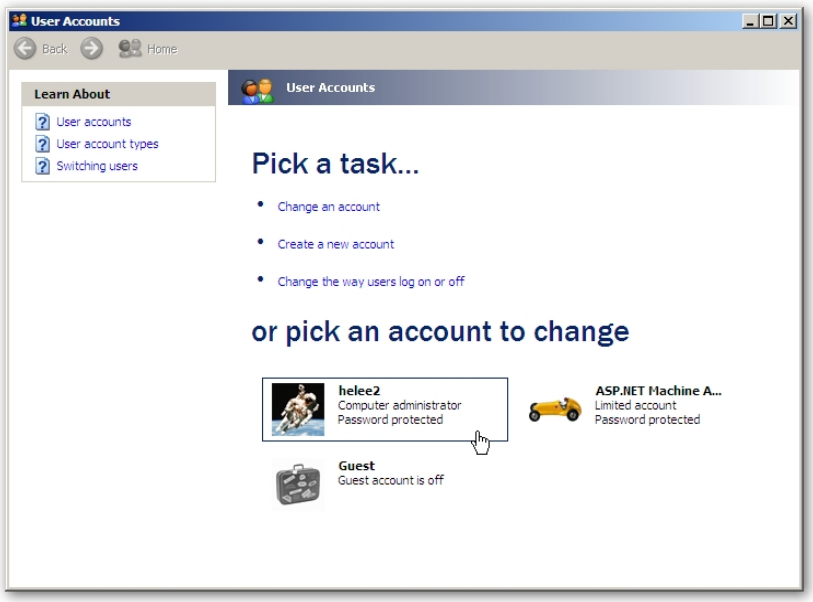


Figure 38: List of accounts in the User Accounts window

3. When your computer account is shown, click on the text that says, "Change my password."

4. Fill out all of the boxes you see in the password change window. If you have trouble remembering your password, you can provide yourself with a hint at the bottom (but make sure that your hint is not your actual password).

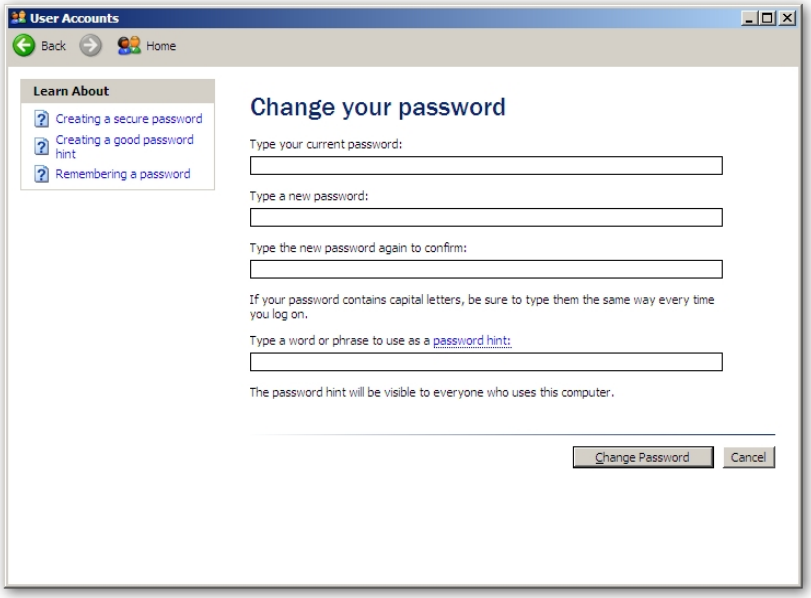


Figure 39: Changing the account password in Windows XP

5. When you're finished, click on "Change Password."

Should I have an Administrator password? How do I create or change it?

Should you have an Administrator password? ***Yes!*** Your computer includes a hidden super-user account, commonly referred to as the "Administrator" account. You don't see it in most cases, because it should only be used when you need to perform unusual administrative tasks (or you can't login to your own account).

An Administrator password is one of the most commonly overlooked parts of computer security. The Administrator account is the one single account that is guaranteed to be present on all Windows computers, ***and*** it will always be able to carry out security-related tasks. It absolutely must have a strong password, and should only be used when absolutely necessary. A computer without an Administrator password is the same as a house with no locks: wide open, and completely vulnerable.

The safest way to set a password for your Administrator account is to open it in Safe Mode. To do so, follow these steps (also outlined in the **"Anti-Virus"** section, on page 7):

1. Turn on or restart your computer.

2. When your computer manufacturer's initial boot-up screen is displayed, begin tapping the "F8" key on your keyboard. (Note: "Windows XP" is ***not*** your manufacturer. It will be the computer manufacturer, such as Dell, HP, Gateway, etc.)

3. If you were successful, you will see a screen similar to the following:

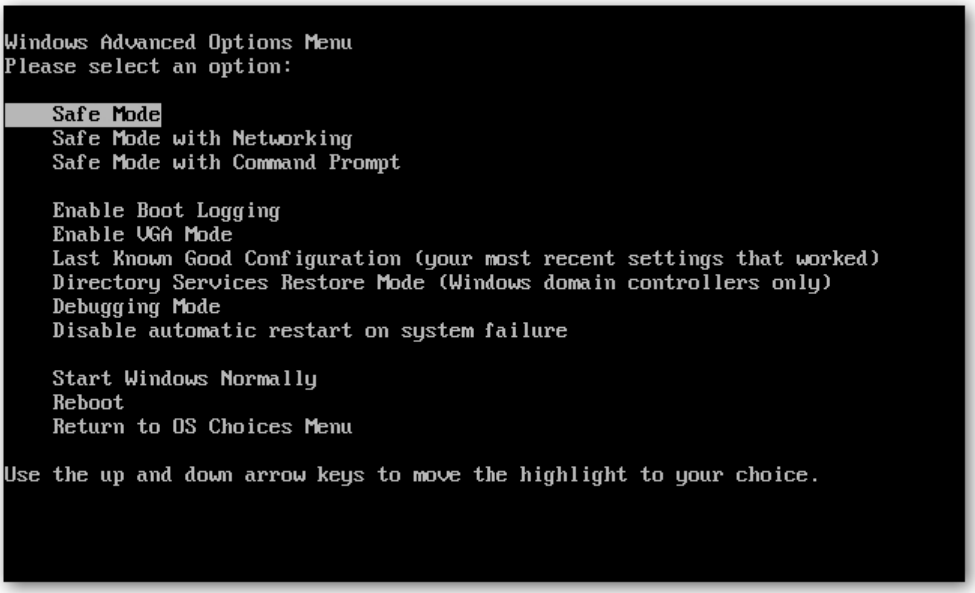


Figure 40: Selecting "Safe Mode" from the menu

4. Use the keyboard arrows to move the cursor up to "Safe Mode," then press Enter. **Do NOT** select "Safe Mode with Networking" or "Safe Mode with Command Prompt."

5. In some cases, you may be prompted to select an operating system. Again, use the keyboard arrows to choose the appropriate selection for your computer, and then press Enter.

6. In a few moments, Safe Mode will open. You may be asked to login. Do so normally, using the same user name and password that you use when accessing your computer. After a few moments, you will see a notification window similar to this:

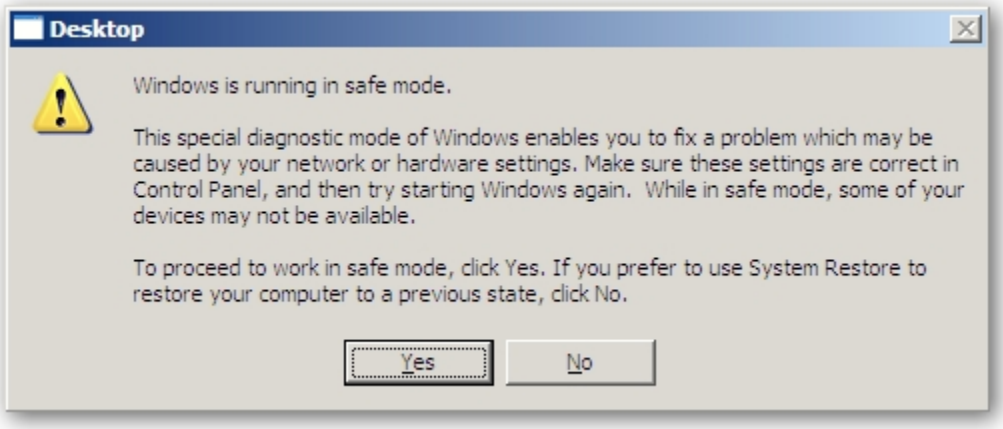


Figure 41: Welcome to Safe Mode

Once you see this notification window, you've entered Safe Mode. From here, use the steps outlined in the section above titled "**How to I change my password on my computer?"** Select the account titled "Administrator" this time, and change the password using the same steps.

How do I change my password for my NCSU Unity account?

To change your Unity account password, visit the following web site:

http://www.ncsu.edu/password

It's important to note here that the password you use with your Unity account must meet certain criteria, in order to insure that it's a "strong" password. The website will list all the important details and requirements needed to create an acceptable password.

Once you've successfully changed your Unity password, wait up to an hour for the new password to take effect.

Backups and Other Good Computer Security Habits

Should I back up my files?

Backing up your documents and files is an easy way to insure that you can recover quickly when trouble strikes. Consider: Even with the best security defenses and regular maintenance, your computer could still stop working. How much worse it would be if you didn't have a backup of your files?

While there is no one "best way" to back up your files, there are several good approaches:

- Occasionally burn a CD or DVD. You should try to limit yourself to documents that you've created yourself (Microsoft Word and Excel files, presentations, pictures, etc.). A typical CD will hold only 700 MB of data, and a DVD will hold up to 4.7 GB of information. Burned discs can be stored for several years and still retain data safely.

- Buy an external hard drive. For a couple of hundred dollars, you can buy a high-capacity external hard drive, which you connect to your computer via a USB cable. If you need something more portable, you could opt to buy a lower-capacity USB keychain disk instead. To perform a backup with one of these drives, simply copy your files from your computer to the external hard drive.

- Automate your backups with software. There are several programs available for PC users that make it easy to back up your important work. Some external drives come with "personal editions" of these programs, which meet the needs of most users.

What else can I do to keep my computer protected?

Laptop users have an additional worry. One of the most basic and often overlooked aspects of security is the physical location of your workstation. Is it sitting in a location where others can easily access it? If the answer to this question is "yes," you're at very high risk for larceny.

By leaving your computer out in the open, you are vulnerable to the most basic breach of security possible: unrestricted physical access to the computer. If someone can touch your computer, and you don't have it locked down with a physical security lock, your computer won't belong to you for very long. Don't take the chance.

Appendix A: Installing and Using Symantec AntiVirus

Symantec AntiVirus is the officially supported anti-virus software solution that NC State University provides to the university community. It is freely available to all students, faculty and staff of the institution, and can be downloaded directly from the ITD Antivirus Resources website:

http://www.ncsu.edu/antivirus

Figure A1: ITD Antivirus Resources Website

Information Technology Division keeps the Antivirus Resources website updated on a regular basis. Because the documentation and how-to guides there are always kept current, you should refer to it for information on how to install and use Symantec AntiVirus.

More generic information about anti-virus software is located on page 3 of this document.

Appendix B: Securing Microsoft Outlook

Microsoft Outlook, part of the Microsoft Office productivity suite, is a popular e-mail client. To use it in a safe and secure fashion, there are a few steps you should take.

Use secure connections:

Microsoft Outlook has the ability to use encryption when sending and receiving your e-mail. This keeps you e-mail password away from prying eyes, and your e-mail safe. To set up a secure connection for your Unity e-mail account, perform the following steps:

1. Open the Tools menu, and select "E-mail Accounts."

2. When the E-mail Accounts window opens, select "View or change existing e-mail accounts," then click on "Next."

3. On the next window, you will see a list of the e-mail accounts in Outlook. Click on your NCSU Unity e-mail account (typically **"unityid.mail.ncsu.edu"** where **unityid** is your Unity user ID). When your account is highlighted, click the "Change" button.

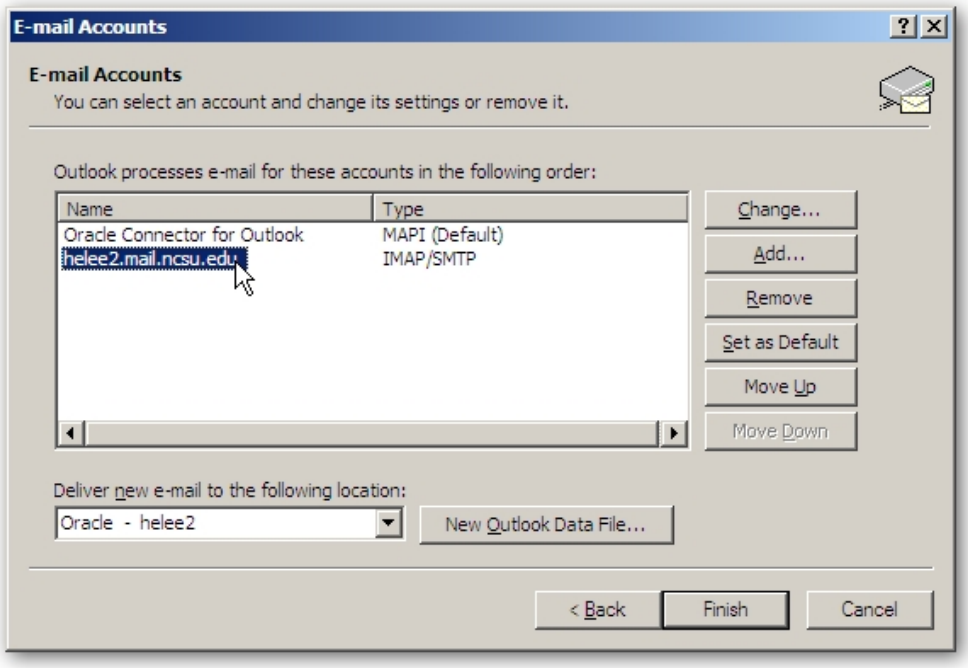


Figure B1: Selecting an e-mail account in Outlook

4. When the account mail settings window appears, click on the "More Settings" button at the bottom of the window.

5. The Internet E-mail Settings window will appear. Click on the "Outgoing Server" tab. Put a check in the box for "My outgoing server (SMTP) requires authentication." Make sure that "Use same settings as my incoming mail server" is selected as well.

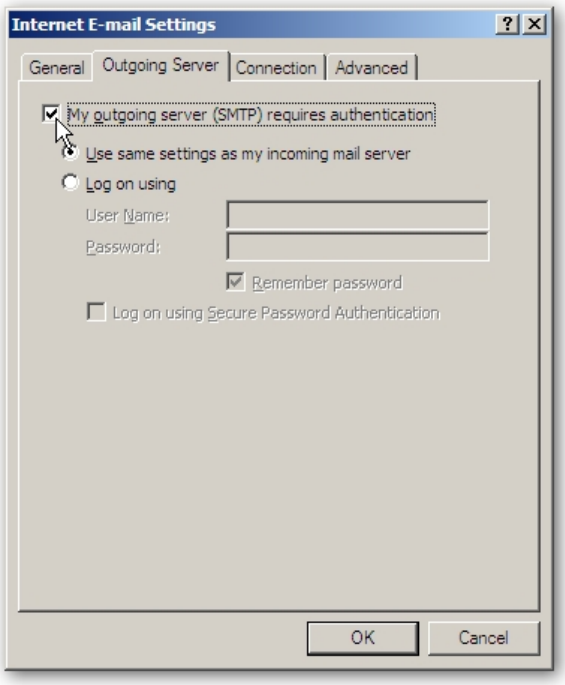


Figure B2: Internet E-mail Settings in Outlook

6. While still in the Internet E-mail Settings window, click on the "Advanced" tab. Put a check in both boxes labeled "This server requires an SSL-secured connection (SSL)." There should be a check mark in both the "Incoming server" and "Outgoing server "sections.

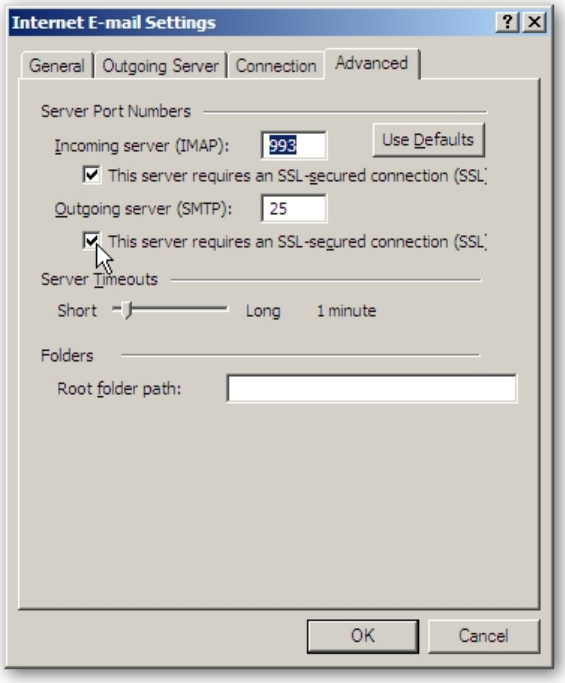


Figure B3: Turning on SSL connections in Outlook

7. You're done. Hit the "OK" buttons in the dialog boxes to return to the main Outlook screen.

Disable JavaScript

Another method to protect your privacy and security is to disable JavaScript. JavaScript, when added to e-mail messages, can have the same harmful effects as if you were to visit a malicious web site. It should be turned off in your e-mail client.

To disable JavaScript in Outlook, take the following steps:

1. Open the Tools menu and select "Options."

2. In the Options dialog box, select the "Security" tab.

3. Look at the Security Zones section and find Zone. Select "Restricted sites" from the list of choices.

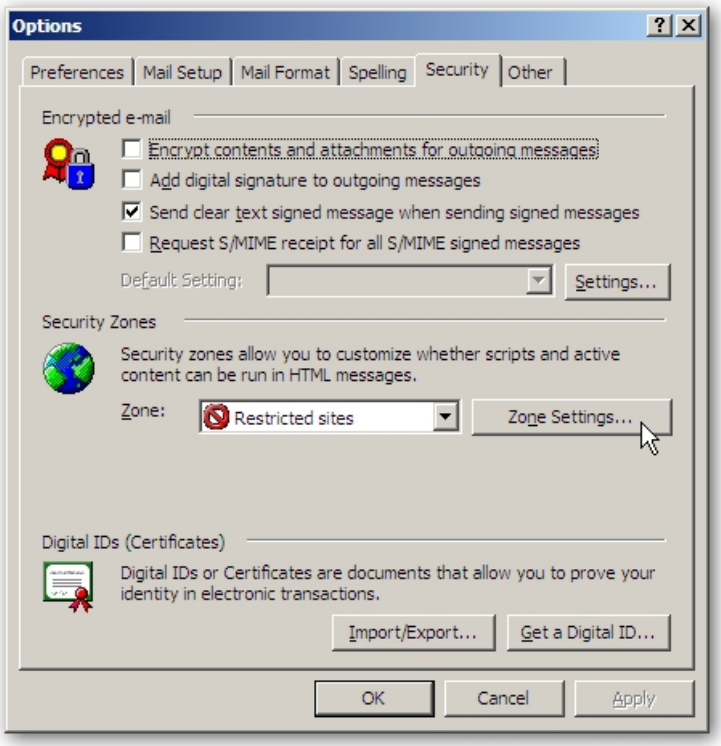


Figure B4: Security tab in Outlook Options

4. Now click on the "Zone Settings" button. Click "OK" when the warning message appears.

5. The Internet Options window that will appear. Make sure that "Restricted sites" is highlighted at the top, and then click on the "Custom Level" button near the bottom.

6. A Security Settings window will appear. Scroll down in the list of settings until you see "Active Scripting" (this section will be very close to the bottom). Please take care not to confuse this with "ActiveX," which appears much higher in the list (close to the top).

7. Change the Active Scripting value to "Disable."

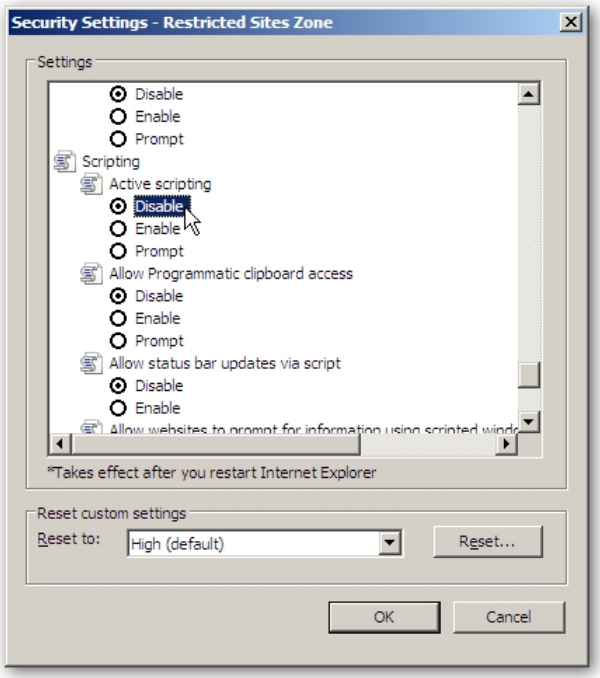


Figure B5: Disabling Active Scripting

8. You're done. Hit the "OK" buttons in the dialog boxes to return to the main Outlook screen.

Disable the Preview Pane:

As an optional extra measure of security, you may wish to turn off the Preview Pane in Outlook. While the preview pane is an easy way to quickly read through your e-mail, the downside is that it can sometimes expose you to unsafe or unwanted e-mail before you have the chance to delete it.

To turn the Preview Pane off in Outlook, go to the View menu and uncheck "Preview Pane."

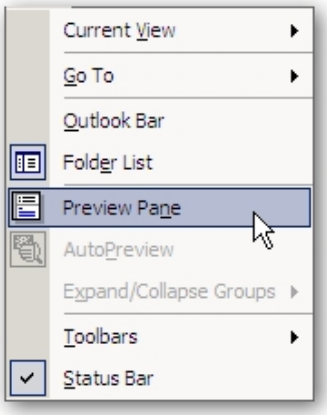


Figure B6: Turning off the Preview Pane in Outlook

Once the Preview Pane is turned off, you will be able to open each message individually by double-clicking, or hitting the "Enter" key when the message is highlighted.

Appendix C: Securing Microsoft Outlook Express

Outlook Express (not to be confused with Microsoft Outlook) is a basic e-mail client that comes with Windows XP. Because of many security problems that have cropped up over the last few years, most information technology professionals will recommend ***against*** using Outlook Express. If you wish to continue using it, there are a few steps you should take to make it safer.

Use secure connections:

Microsoft Outlook Express has the ability to use encryption when sending and receiving your e-mail. This keeps you e-mail password away from prying eyes, and your e-mail safe. To set up a secure connection for your Unity e-mail account, perform the following steps:

1. Open the Tools menu, and select "Accounts."

2. When the Internet Accounts window opens, select the "Mail" tab.

3. You will see a list of the e-mail accounts in Outlook Express. Click on your NCSU Unity e-mail account. In most cases, your NCSU e-mail account will be named something along the lines of **"unityid.mail.ncsu.edu"** (where **unityid** is your Unity user ID).

4. When your account is highlighted, click the "Properties" button.

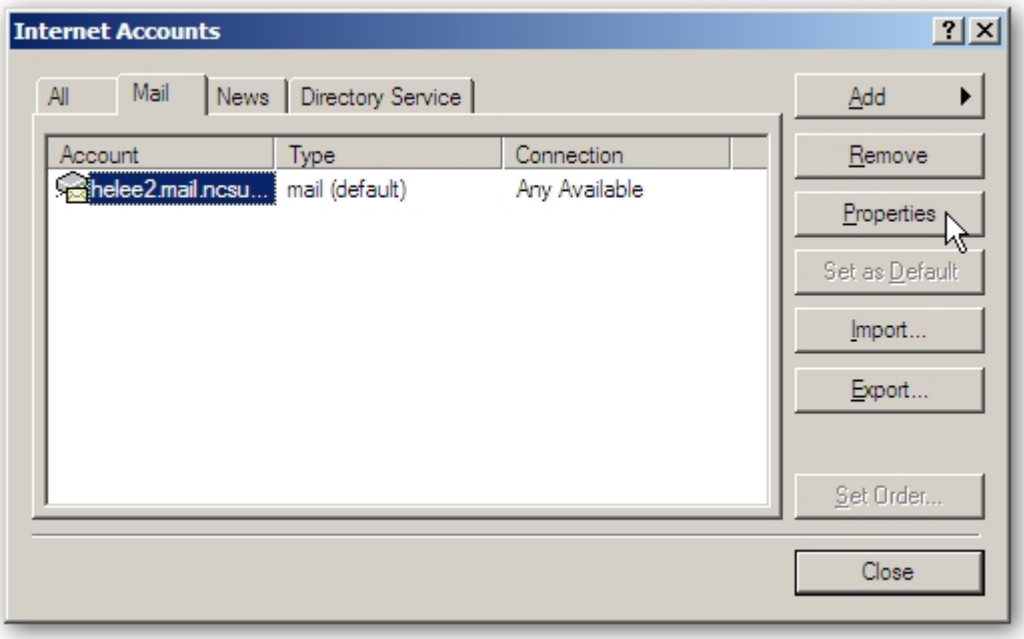


Figure C1: Selecting an e-mail account in Outlook Express

5. An account properties window will appear. Click on the "Servers" tab.

6. Under the "Outgoing Mail Server" heading, put a check in the box for "My server requires authentication."

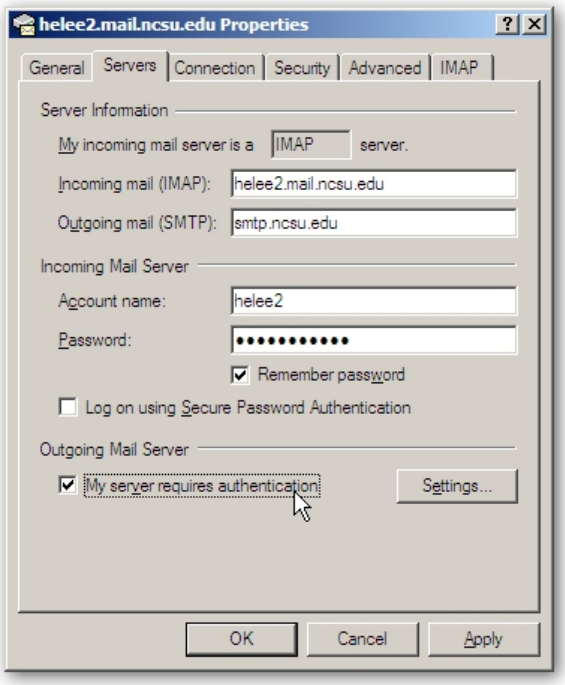


Figure C2: Server Settings in Outlook Express

7. While still in the account properties window, click on the "Advanced" tab. Put a check in both boxes labeled "This server requires an SSL-secured connection (SSL)." There should be a check mark in both the "Incoming server" and "Outgoing server "sections.

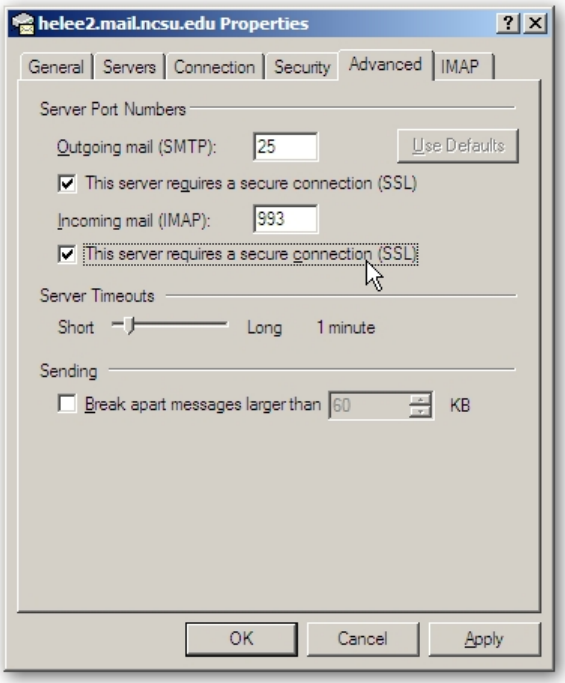


Figure C3: Turning on SSL connections in Outlook Express

8. You're done. Hit the "OK" buttons in the dialog boxes to return to the main Outlook screen.

Disable JavaScript

Another method to protect your privacy and security is to disable JavaScript. JavaScript, when added to e-mail messages, can have the same harmful effects as if you were to visit a malicious web site. It should be turned off in your e-mail client.

To disable JavaScript in Outlook Express, take the following steps:

1. Open the Tools menu and select "Options."

2. In the Options dialog box, select the "Security" tab. Look under the "Virus Protection" section, and select "Restricted sites zone (more secure)." When finished, hit the "OK" button.

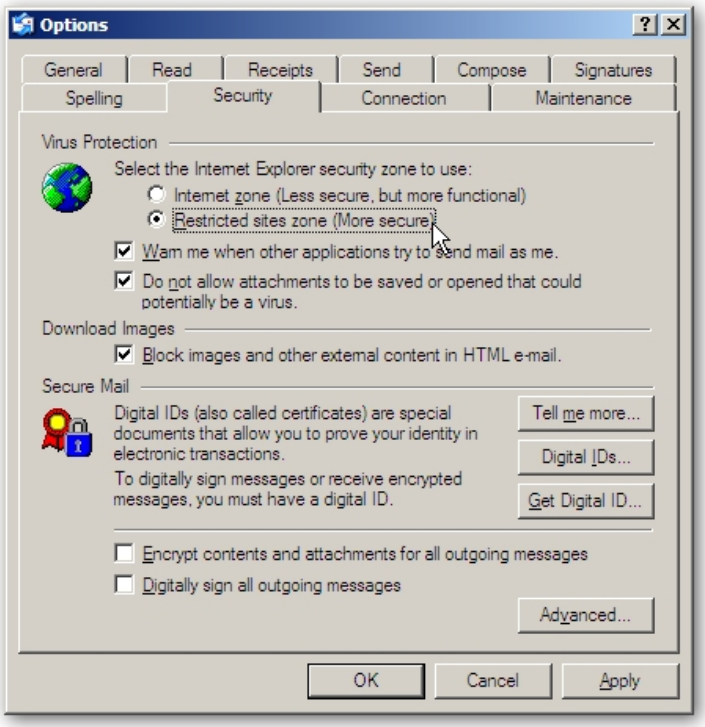


Figure C4: Security tab in Outlook Express Options

3. Next, go to your Start menu and open the Control Panel. Double-click "Internet Options."

Figure C5: Internet Options icon

4. The Internet Options window that will appear. Select the "Security" tab.

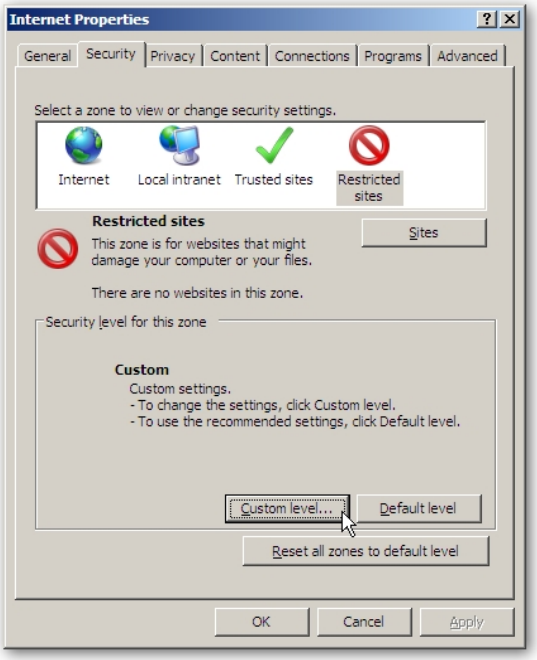


Figure C6: Security tab in the Internet Options window

5. Select the "Restricted sites" icon at the top, and then click on the "Custom Level" button.

6. A Security Settings window will appear. Scroll down in the list of settings until you see "Active Scripting" (this section will be very close to the bottom). Please take care not to confuse this with "ActiveX," which appears much higher in the list (close to the top). Change the Active Scripting value to "Disable."

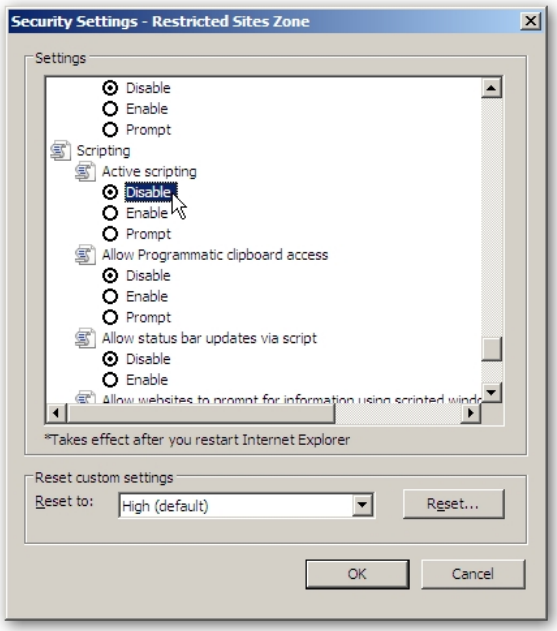


Figure C7: Disabling Active Scripting

7. You're done. Hit the "OK" buttons in the dialog boxes.

Disable the Preview Pane:

As an optional extra measure of security, you may wish to turn off the Preview Pane in Outlook Express. While the preview pane is an easy way to quickly read through your e-mail, the downside is that it can sometimes expose you to unsafe or unwanted e-mail before you have the chance to delete it.

To turn the Preview Pane off in Outlook Express, go to the View menu and select "Layout." In the Window Layout Properties dialog box, uncheck the box next to "Show preview pane."

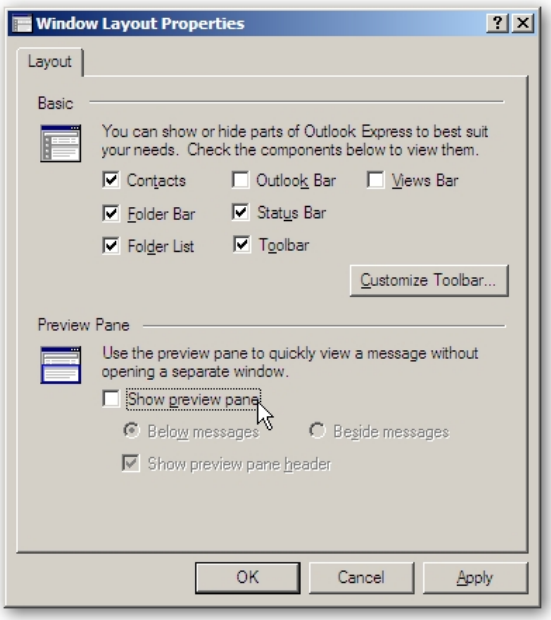


Figure C8: Turning off the Preview Pane in Outlook Express

Once the Preview Pane is turned off, you will be able to open each message individually by double-clicking, or hitting the "Enter" key when the message is highlighted.

Appendix D: Securing Mozilla Thunderbird

Mozilla Thunderbird is a free e-mail client, written by the same company that produces the Firefox web browser. To use it in a safe and secure fashion, there are a few steps you should take.

Use secure connections:

Thunderbird has the ability to use encryption when sending and receiving your e-mail. This keeps you e-mail password away from prying eyes, and your e-mail safe. To set up a secure connection for your Unity e-mail account, perform the following steps:

1. Open the Tools menu, and click on "Account Settings."

2. In the Account Settings window, locate your NCSU Unity e-mail account from the list on the left side. In most cases, your NCSU e-mail account will be named something along the lines of **"unityid.mail.ncsu.edu"** (where **unityid** is your Unity user ID).

3. Under your NCSU account in the list, click on "Server Settings." A list of server options will appear on the right. In the "Security Settings" section, select "SSL."

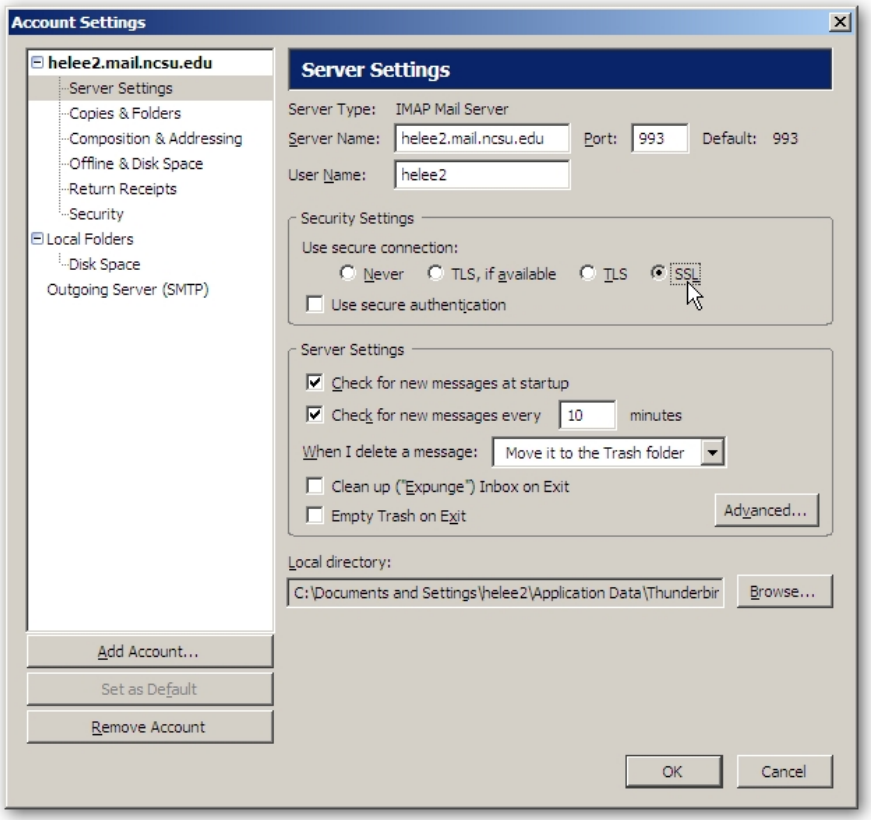


Figure D1: Server Settings in Thunderbird

4. Next, look at the bottom of the list on the left, and select "Outgoing server (SMTP)." You should see your outgoing mail server listed on the right. Select your server and hit "Edit."

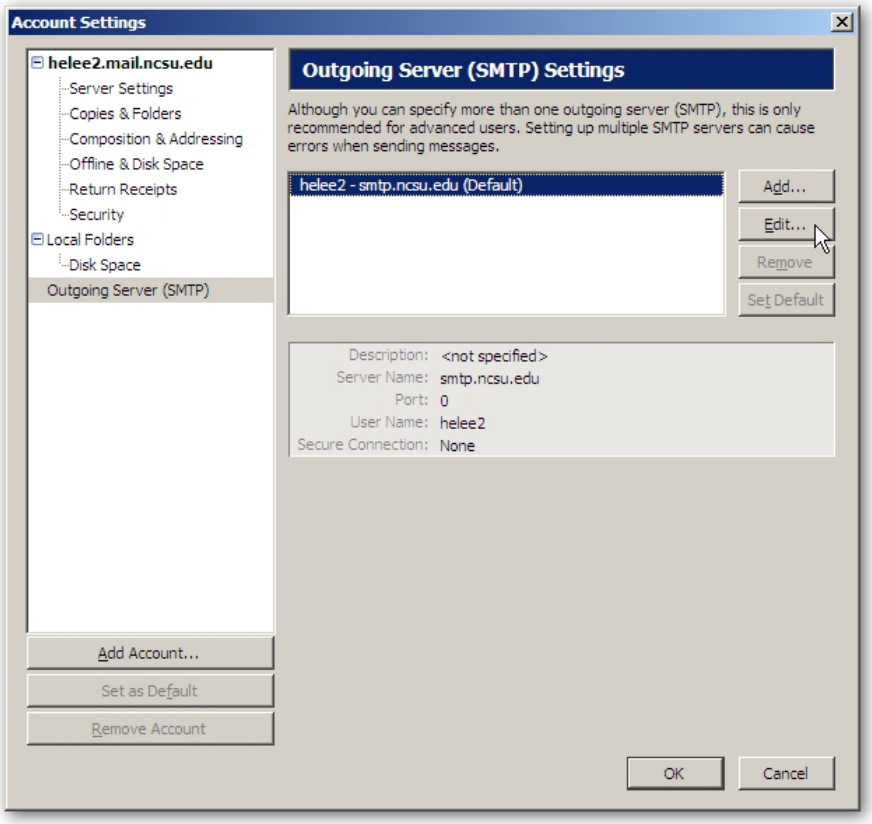


Figure D2: Outgoing mail server list in Thunderbird

5. An SMTP Server window should appear. Make sure that your Unity user ID is listed in the "User Name" box. Below that, for "Use secure connection," select "TLS."

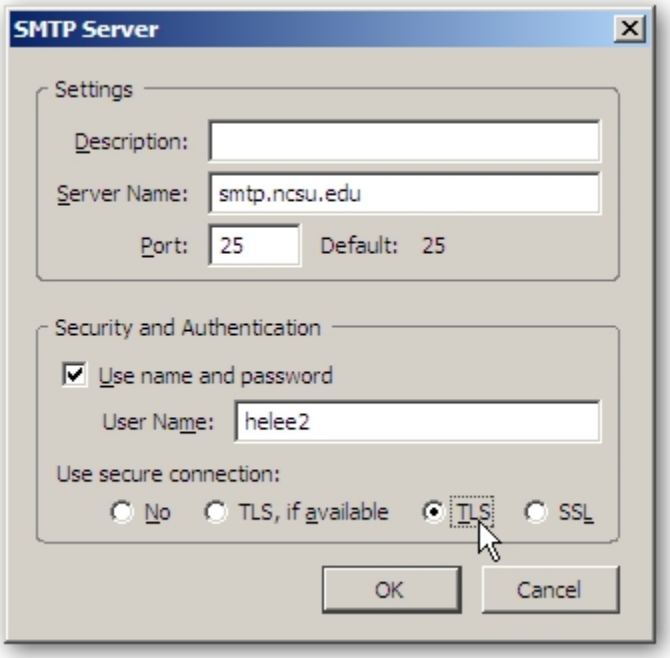


Figure D3: SMTP server settings in Thunderbird

6. Click OK to close the SMTP Server window, and then click OK again to close the Account Settings window.

7. Close Thunderbird, and then open it again.

8. When Thunderbird opens again, you may be prompted to install a security certificate. This helps you to insure that your connection to the e-mail server is secure. Click on "Accept this certificate permanently," and then click the "OK" button.

Figure D4: Being prompted to install a security certificate in Thunderbird

9. You're done. Your connections to the e-mail server are now secure.

Disable JavaScript

Another method to protect your privacy and security is to disable JavaScript. JavaScript, when added to e-mail messages, can have the same harmful effects as if you were to visit a malicious web site. It should be turned off in your e-mail client.

To disable JavaScript in Thunderbird, take the following steps:

1. Open the Tools menu, and click on "Options."

2. The Options dialog box will appear. Click on the "Privacy" icon at the top.

3. You will see several privacy- and security-related options here. Make sure that the "General" tab is selected.

4. Look for the checkbox labeled "Block JavaScript in mail messages," and make sure that it is checked (it should already be checked by default).

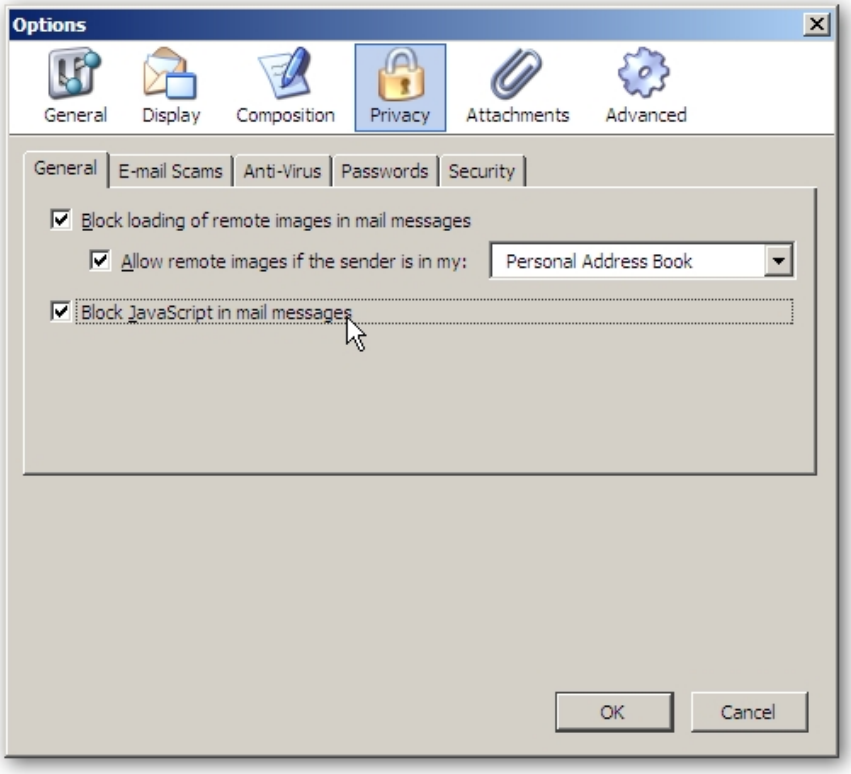


Figure D5: Blocking JavaScript in Thunderbird

Disable the Message Pane:

As an optional extra measure of security, you may wish to turn off the Message Pane in Thunderbird. While this message preview pane is an easy way to quickly read through your e-mail, the downside is that it can sometimes expose you to unsafe or unwanted e-mail before you have the chance to delete it.

To turn the Message Pane off in Thunderbird, go to the View menu, open the Layout sub-menu, and select "Message Pane." You can also turn the Message Pane off and on by pressing the F8 function key on your keyboard.

Once the Message Pane is turned off, you will be able to open each message individually by double-clicking, or hitting the "Enter" key when the message is highlighted.

Appendix E: Using Microsoft Windows Defender

Windows Defender is a free anti-spyware product from Microsoft. Recently released as an add-on feature for Windows, this anti-spyware scanner is a very effective tool against spyware and adware threats. It can be obtained from Microsoft's website:

http://www.microsoft.com/athome/security/spyware/software/default.mspx

If you choose to download and install Windows Defender, make sure that you select **"Use recommended settings"** during the installation process:

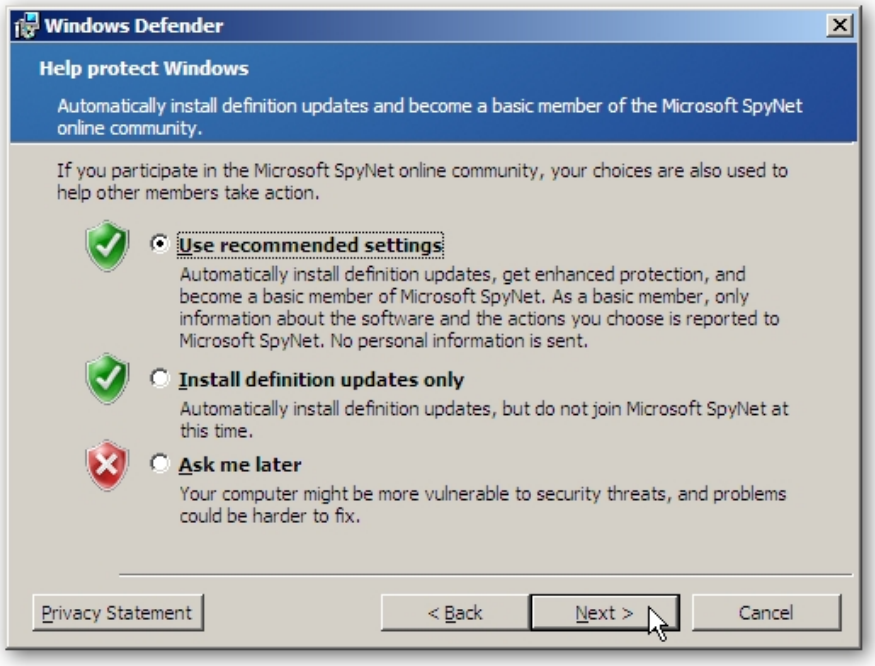


Figure E1: Installation of Windows Defender

When the installation is finished, you will be invited to let Windows Defender download anti-spyware definitions and to run a quick scan of your computer. You should let it do so, so you can receive immediate protection.

Scanning for spyware/adware with Windows Defender:

To use Windows Defender to scan your computer for spyware and adware:

1. Open your Start menu, click on "All Programs," then locate and select Windows Defender.

2. Windows Defender will launch. If it has not been updated in a while, you will see an on-screen prompt to let it connect to the Internet and download fresh spyware definition files. This process can sometimes take several minutes, so be patient while it works.

3. At the top of the Windows Defender screen, click the icon labeled "Scan."

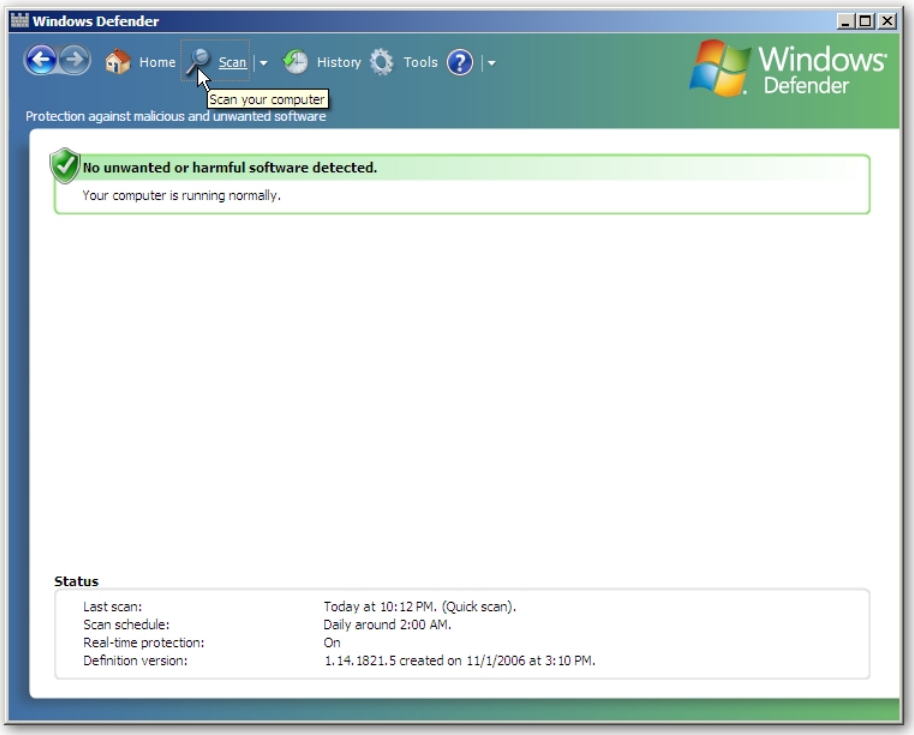


Figure E2: Microsoft Windows Defender

4. Windows Defender will begin a "quick scan" of your hard drive. A "quick scan" will look in the locations on your computer where spyware and adware most commonly install themselves. The scan may take several minutes, depending on your computer's speed and number of files.

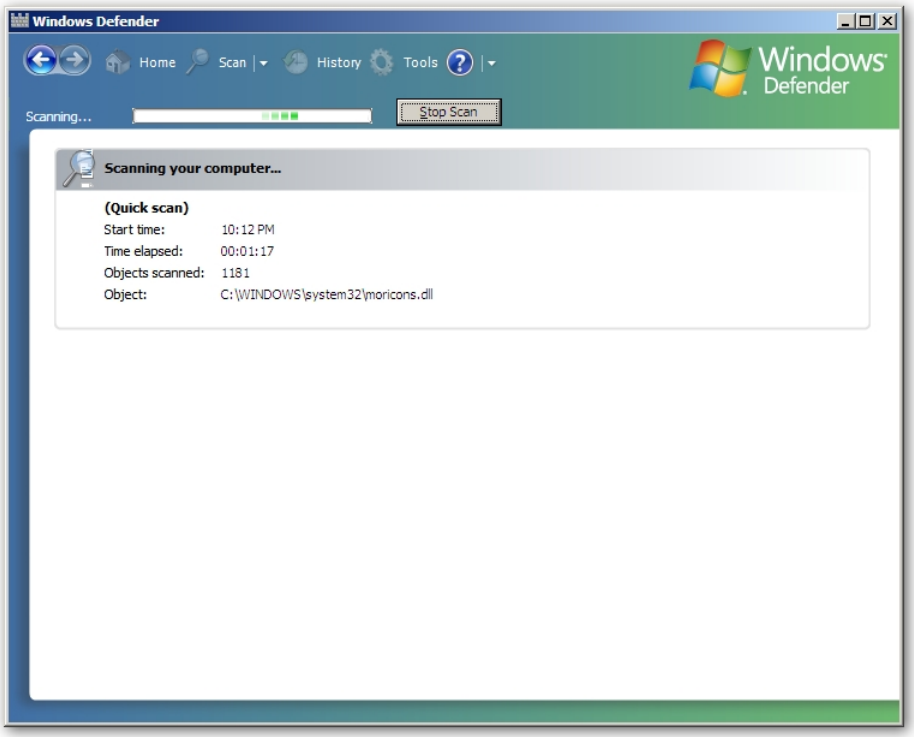


Figure E3: Windows Defender performing a spyware scan

5. When the spyware scan is complete, Windows Defender will display a results screen. If it does not detect any spyware components on your computer, you will get a clean bill of health:

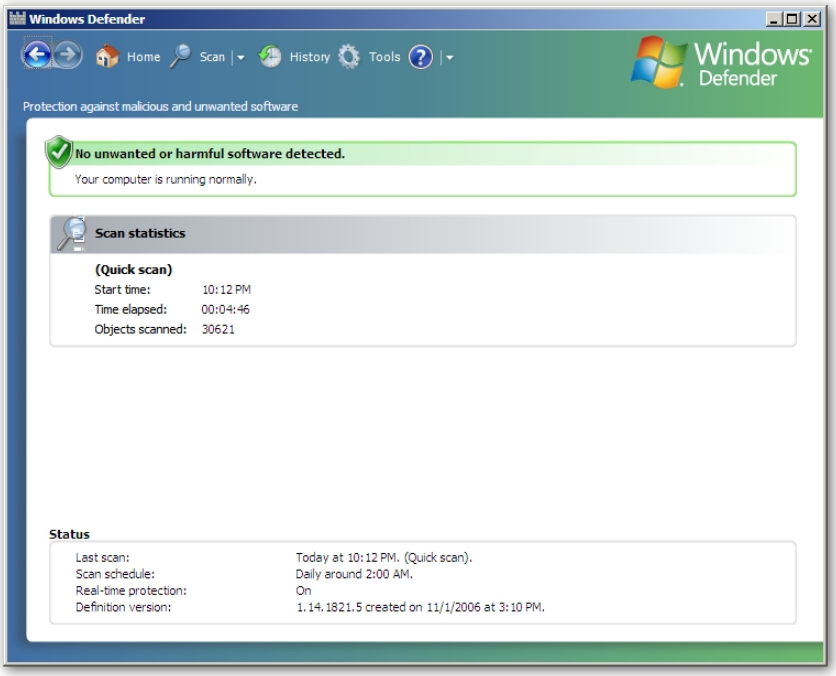


Figure E4: Scan completed in Windows Defender with no spyware

If spyware or adware is found, you will be prompted to remove it:

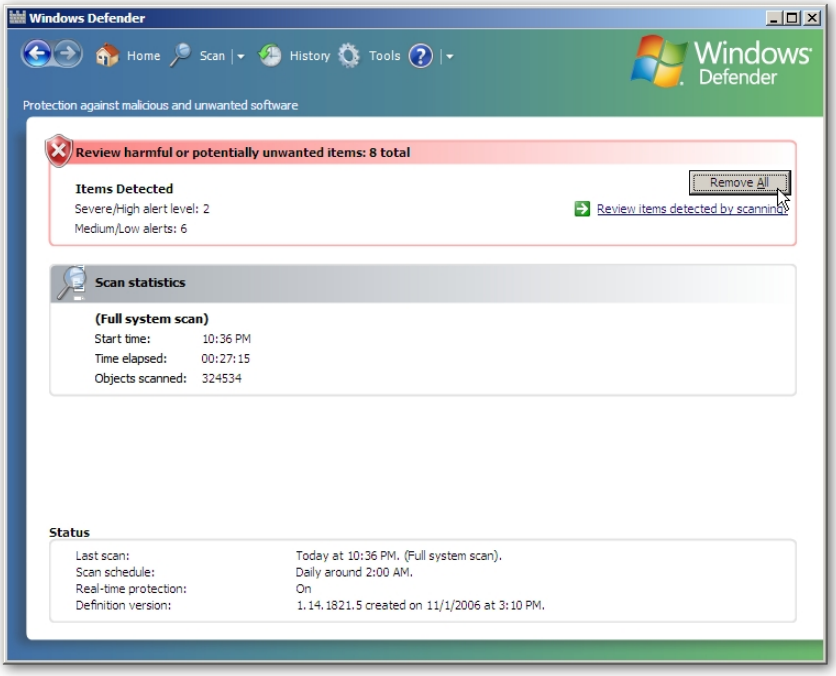


Figure E5: Windows Defender finds spyware threats

The advice Windows Defender gives for what to remove, and what not to remove, is typically accurate and safe to reply upon. In some cases, you may wish to review the list of items that Windows

Defender plans to delete or modify. To see the list of probable spyware/adware threats found by Windows Defender, click on the link titled "Review items detected by scanning:"

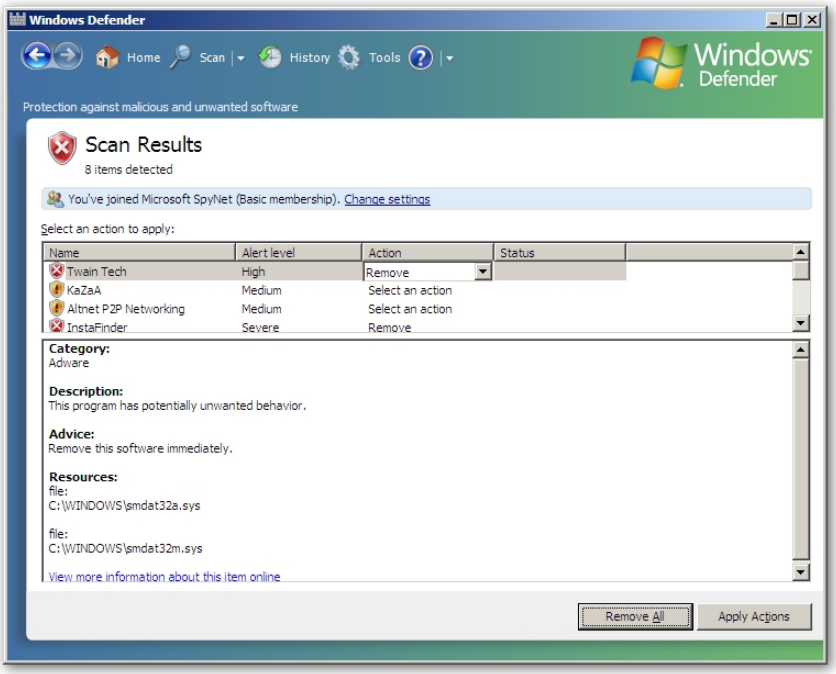


Figure E6: Full list of spyware/adware found by Windows Defender

6. If you're prompted to restart your computer to complete the removal of spyware, do so immediately or as soon as possible.

You may find that you have better success in removing spyware and adware programs if you perform your anti-spyware scan in Safe Mode. For more information on how to open Safe Mode on your computer, see the **Viruses and Anti-Virus Software** section titled **"How do I run an anti-virus scan?"**

How to I turn on the real-time background anti-spyware protection in Windows Defender?

Windows Defender includes an anti-spyware defense that runs in the background on your computer at all times. This real-time protection can help prevent spyware and adware programs from becoming installed on your machine.

Tip: As with anti-virus programs, you should run only one anti-spyware program in the background at a time. You can have several anti-spyware programs installed on your computer, but only one should run at a time. Multiple anti-spyware programs, running simultaneously, can cause system errors.

To turn on the real-time protection in Windows Defender, take the following steps:

1. Open your Start menu, click on "All Programs," then locate and select Windows Defender.

2. Windows Defender will launch. Click on the "Tools" icon at the top of the window.

3. The Tools menu will appear. Click on the icon labeled "Options."

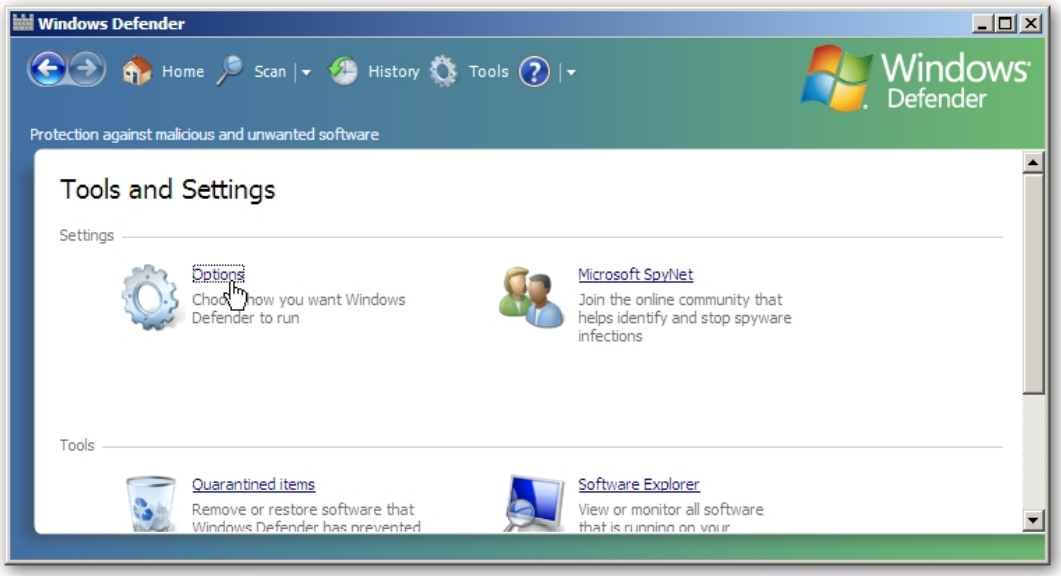


Figure E7: Options icon in the Windows Defender Tools menu

4. Scroll down to the section titled "Real-time protection options." You should see several checkboxes under this heading. Place a check in the box for "Use real-time protection (recommended)."

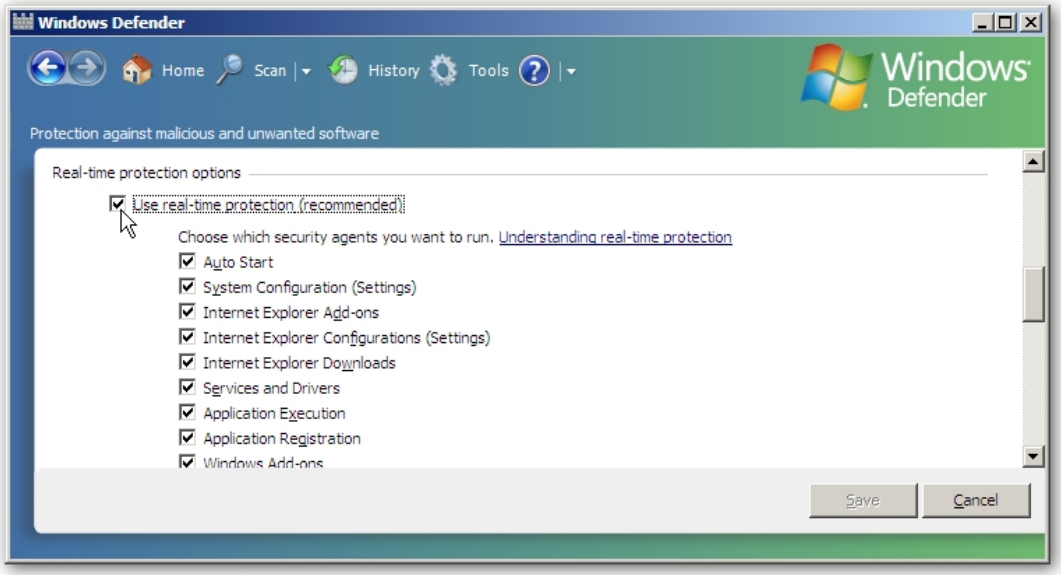
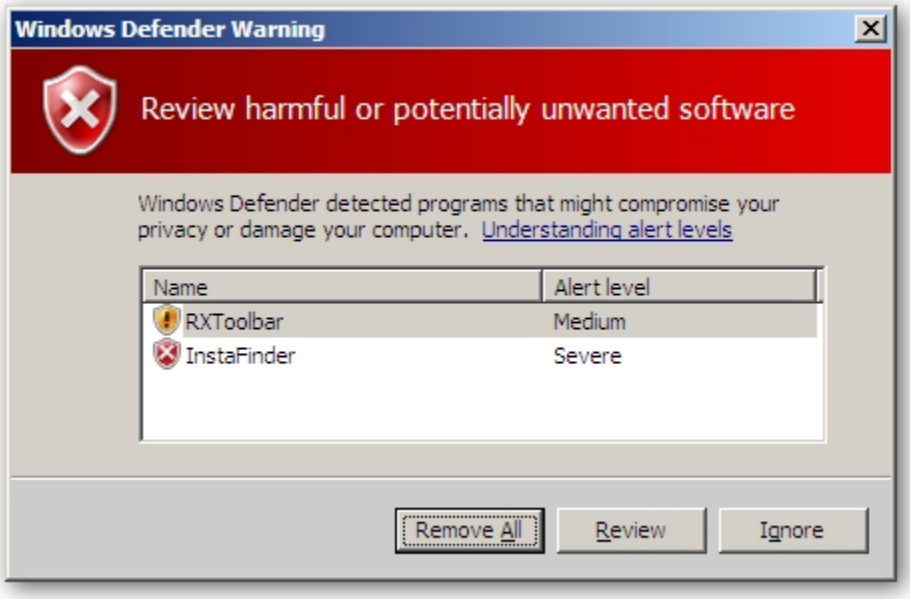


Figure E8: Turning on real-time protection in Windows Defender

5. Click the "Save" button to save the change you made. Real-time background anti-spyware protection has been enabled.

When Windows Defender's real-time background protection is running, you may occasionally see alert windows like this, letting you know that it needs your attention:



E9: Windows Defender security warning

This alert lets you know that, just like with an anti-virus scanner, a threat has been detected, and you need to take action immediately. You can review information about the threats Windows Defender discovered, and remove them accordingly.

Appendix F: Using Spybot – Search & Destroy

Spybot – Search & Destroy is a free anti-spyware product. It can be obtained from the following website:

http://www.safer-networking.org/en/index.html

Spybot S&D offers a wealth of anti-spyware tools and protections, and can be configured for use by both inexperienced and advanced users. However, if you're a first-time anti-spyware user, you may wish to look first at Microsoft Windows Defender (see **Appendix E** for additional details), as it is geared more towards the common computer user. If you are an advanced computer user and don't mind a little complexity, Spybot S&D may be better suited to your needs.

If you choose to download and install Spybot S&D, make sure that you select **"Download updates immediately"** during the installation process. Choosing this option will allow the installer program to connect to the Internet and obtain program updates before it even begins to load Spybot S&D on your computer.

You may also be prompted to install "Internet Explorer protection (SDHelper)" and "System settings protection (TeaTimer):"

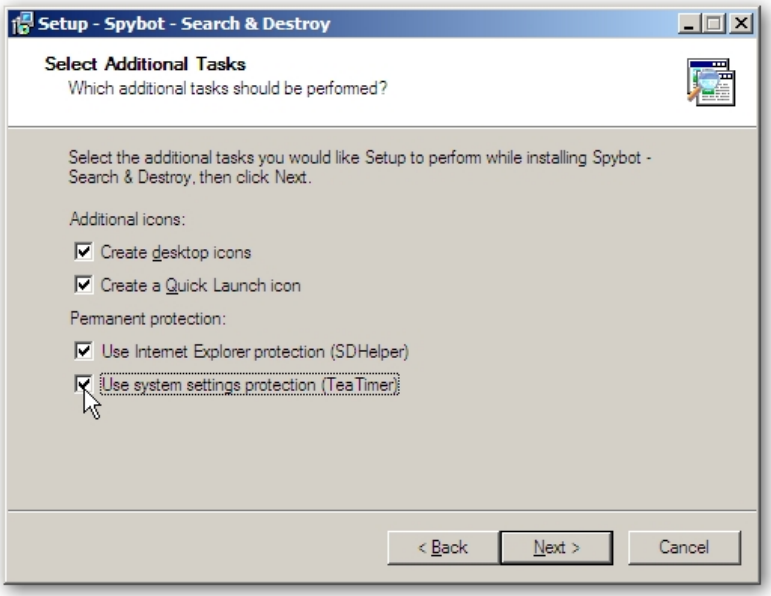


Figure F1: Installation options for Spybot – Search & Destroy

SDHelper is a very useful tool to have installed on your computer, as it will block some unsafe downloads in Windows Internet Explorer. TeaTimer is also nice to have, but ***only*** if you are not already running an anti-spyware program in the background (see **How do I turn on the real-time background protection in Spybot S&D**, below, for more information).

When the installation is finished, you will be invited to let Spybot S&D to launch, and go through the initial configuration wizard. You should let it do so, and follow the suggestions it makes.

Once Spybot S&D is open, you will initially see its "Default" display mode. Spybot S&D has two display modes, which you can choose in the "Mode" menu:

- **Default Mode:** In Default Mode, Spybot S&D will show you the most common anti-spyware options and tools. This mode is good for standard users.

- **Advanced Mode:** In Advanced Mode, you have access to the complete set of anti-spyware utilities in Spybot S&D. This mode will likely intimidate inexperienced users.

Scanning for spyware/adware with Spybot – Search & Destroy:

To use Spybot S&D to scan your computer for spyware and adware:

1. Open your Start menu, click on "All Programs," then locate and select "Spybot – Search & Destroy."

2. Spybot S&D will launch. If it has not been updated in a while, you can hit the "Search for Updates" button to have the program update itself.

3. Click the button labeled "Check for problems."

Figure F2: Spybot – Search & Destroy

4. Spybot S&D will begin a scan of your hard drive. The scan may take several minutes, depending on your computer's speed and number of files.

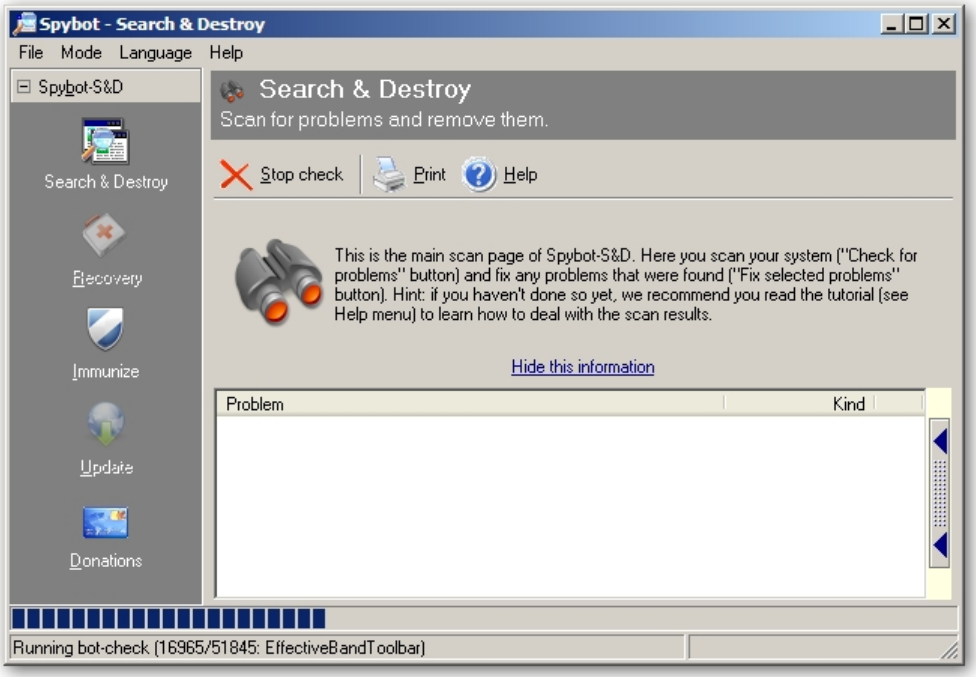


Figure F3: Spybot S&D performing a spyware scan

5. When the spyware scan is complete, Spybot S&D will display a results screen. If it does not detect any spyware components on your computer, you will get a clean bill of health:

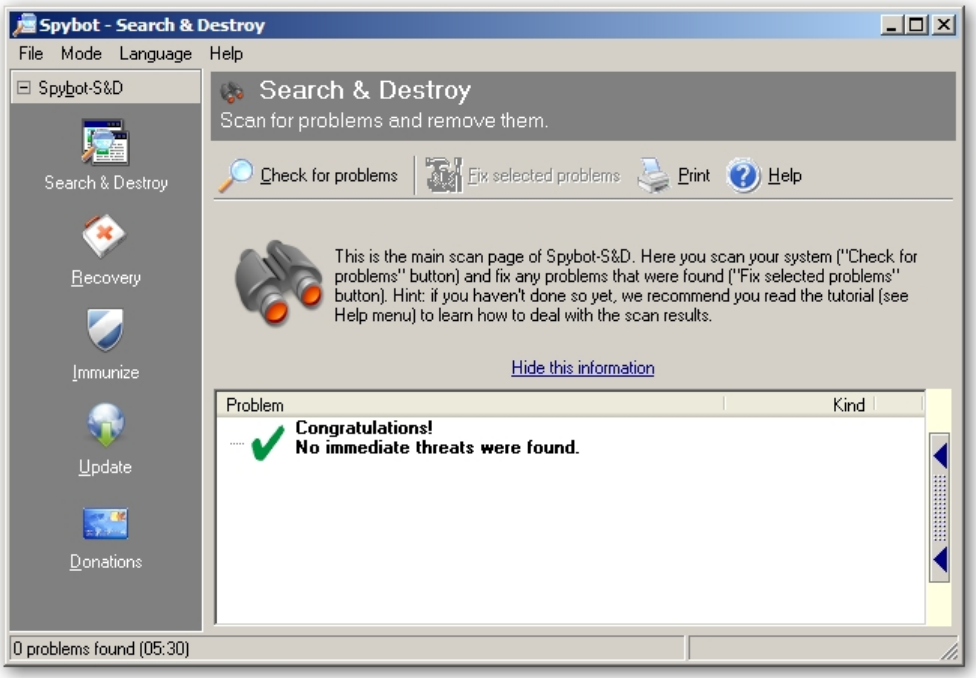


Figure F4: Scan completed in Spybot S&D with no spyware

If spyware or adware is found, you will be prompted to remove it:

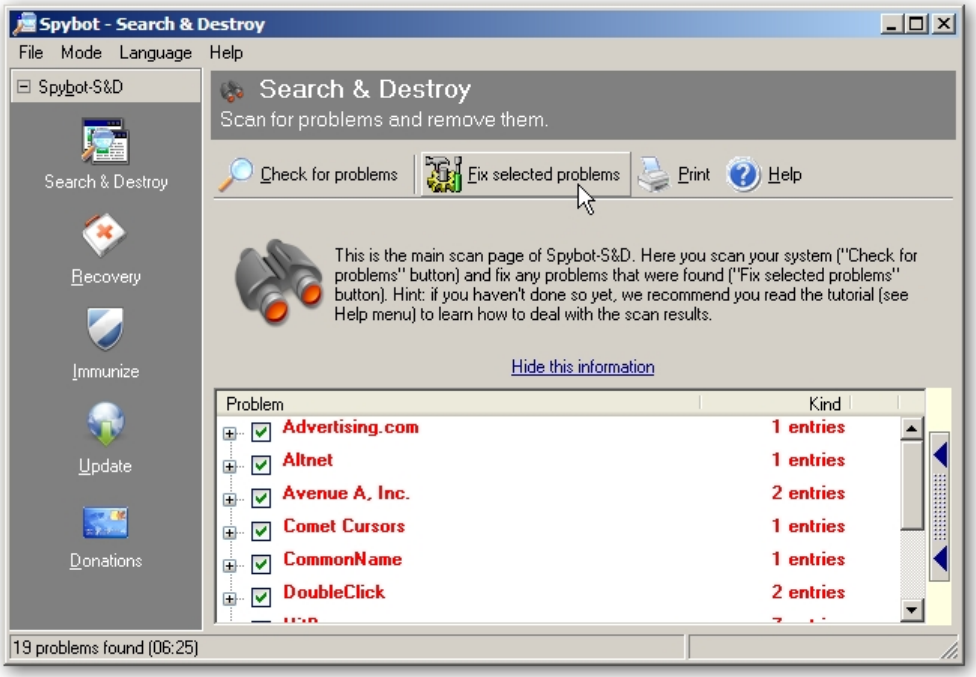


Figure F5: Spybot S&D finds spyware threats

The advice Spybot S&D gives for what to remove, and what not to remove, is typically accurate and safe to reply upon. If you wish to review the list of items that Spybot S&D plans to delete or modify, you can click on the individual plus icons to the right of the listed.

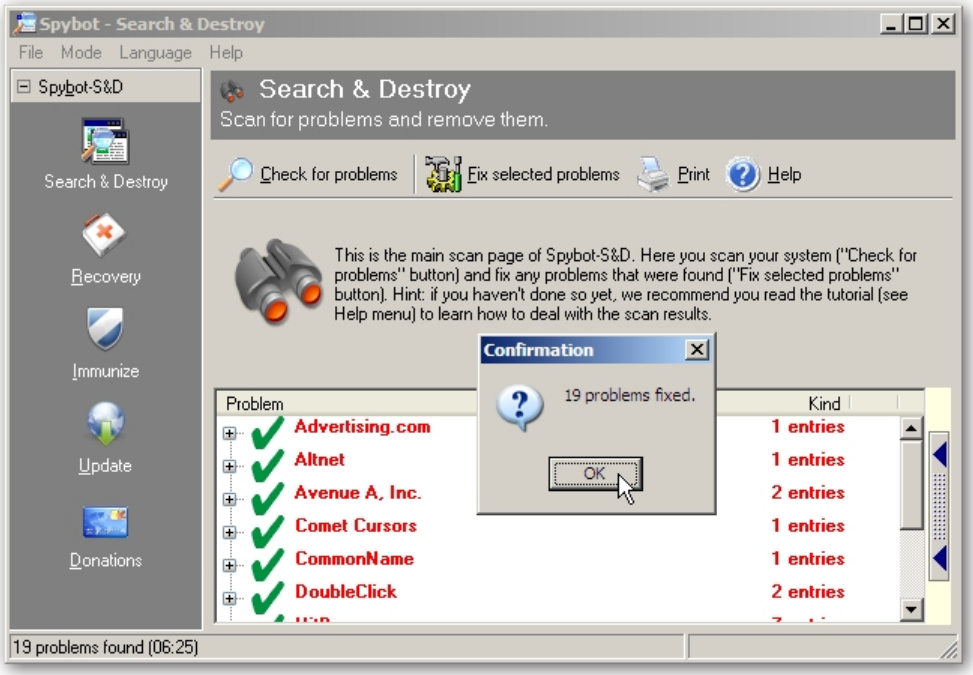


Figure F6: Spybot S&D cleans up spyware threats

6. If you're prompted to restart your computer to complete the removal of spyware, do so immediately or as soon as possible.

You may find that you have better success in removing spyware and adware programs if you perform your anti-spyware scan in Safe Mode. For more information on how to open Safe Mode on your computer, see the **Viruses and Anti-Virus Software** section titled **"How do I run an anti-virus scan?"**

How to I turn on the real-time background anti-spyware protection in Spybot S&D?

Spybot – Search & Destroy includes two anti-spyware defenses that run in the background on your computer at all times. The first, called "SDHelper," protects you by restricting unsafe or malicious downloads in Windows Internet Explorer. The second, called "TeaTimer," this real-time protection can help prevent spyware and adware programs from becoming installed on your machine. These two programs, running together, provide an excellent defense against most common types of spyware and adware infections.

As was stated above, SDHelper is safe to run in combination with other anti-spyware programs. TeaTimer users should be careful not to use multiple anti-spyware real-time background scanners.

Tip: As with anti-virus programs, you should run only one anti-spyware program in the background at a time. You can have several anti-spyware programs installed on your computer if you wish, but you should allow only one to run at a time. Multiple anti-spyware programs, running simultaneously, can potentially cause system errors.

To turn on the real-time protection in Spybot S&D, take the following steps:

1. Open your Start menu, click on "All Programs," and then select Spybot – Search & Destroy.

2. Spybot S&D will launch. Click on the "Mode" menu, and then click on "Advanced."

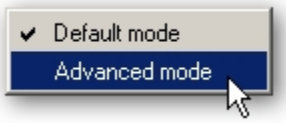


Figure F7: Mode menu in Spybot S&D

3. You may receive a warning prompt. Click "Yes" to continue to Advanced Mode.

4. You will see several additional toolbars at the bottom left of the Spybot S&D window. One of these will be labeled "Tools." Click on it, and the tools list will appear.

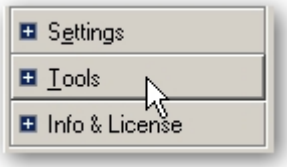


Figure F8: Tools toolbar at the bottom left of the Spybot S&D window

5. With the tools list open, look for the icon labeled "Resident," and click.

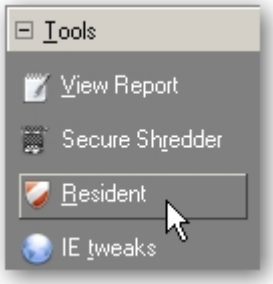


Figure F9: Tools list in Spybot S&D

6. The Resident options menu will appear on the right. Place checks in the checkboxes for both options, **"Resident 'SDHelper"** and **"Resident 'TeaTimer.'"**

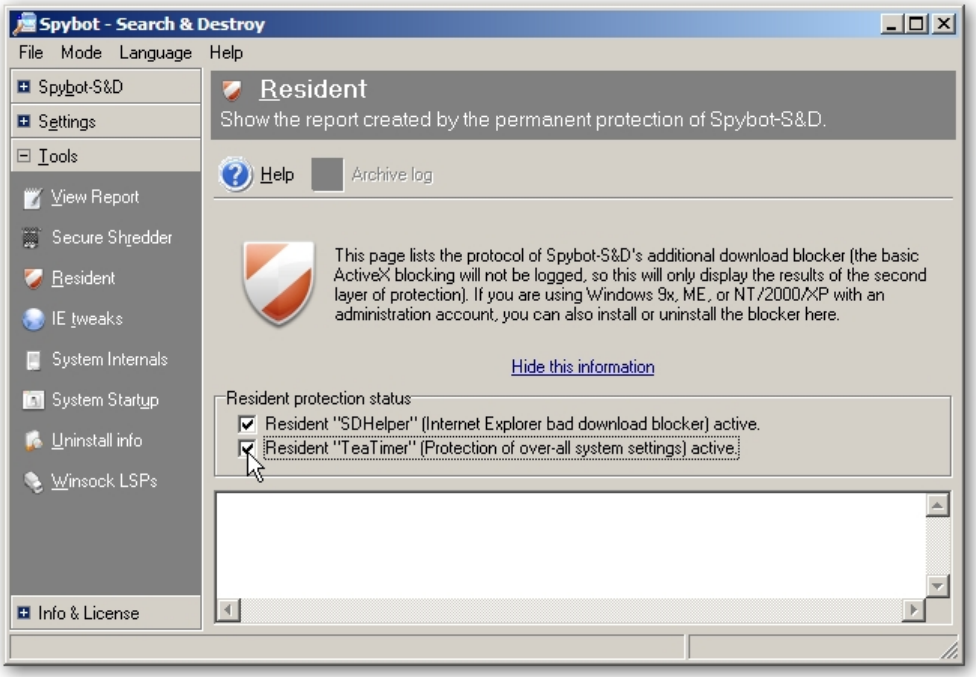


Figure F10: Resident options in Spybot S&D

That's all there is. Real-time background anti-spyware protection has been enabled.

When Spybot S&D's real-time background protection is running, you may occasionally see alert windows, letting you know that it needs your attention. These alerts let you know that, just like with an anti-virus scanner, threats have been detected, and you need to take action immediately. You can review information about the spyware/adware discovered and react it accordingly.