



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Christina Klam

GSEC Practical Requirement: V. 1.4b

Mentor with Sudha Sudanthi

Background on Paper:

I never planned on writing this paper. However, in August 2003, two things happened that changed the direction of my paper topic. The MS Blaster & Sobig viruses were one. My mother getting a cable modem was the other. Between my mother, my friends, and their friends, I barely spent an evening at home all of August. It seemed that everyone was hit by either of these viruses or were terrified that they were “next.” While the viruses affected many businesses, I feel it was the home users who felt the most lost. As my friend Barbara said, “I tried to do what Microsoft suggested but I didn’t understand what it was telling me to do.” When I went online to find them a user-friendlier, yet informative set of directions, I was disappointed. While there are many good papers out there, there is not one that truly fits the needs of my friends and family. So I decided to write one—a paper that explains what computer security risks exist and how to address them.

Defense in-Depth: Protection from the Deluge of Internet Dangers

Remember back when you were stuck outside during in a huge rainstorm? You had an umbrella. While the umbrella was adequate in the beginning, it just wasn’t enough when it began to storm. The umbrella was only able to keep your head dry. What about your legs and feet or your bag? To stay completely dry, you would have had to wear galoshes to keep your feet dry, rubber overalls to keep your legs from getting soaked, and a poncho to protect your upper body and bags.

That is called Defense in-Depth. In terms of computers, it means do not trust just one thing to protect from every intruder, virus, or worm raining down through your internet connection. So, just as an umbrella cannot shield you from every raindrop, neither can a firewall. You still need the “poncho” to guard against saturation of viruses, worms, and Trojan. “Galoshes” to keep the spyware and adware from soaking your feet and the “overalls” to protect/patch over any place left vulnerable to the rain.

As Cole, Fossen, Northcutt, Pomeranz state:

The concept of Defense in-Depth can be applied to different types of networks, at the office as well as at home. For example, if you were putting together a one network, you might use a basic firewall built into your cable modem/DSL router to guard against direct attacks from the

Internet. However, the firewall cannot protect you against all threats. For instance, you may receive a virus via an infected document that was e-mailed to you or handed to you on a floppy. It would be a good idea to install anti-virus software on your workstations to account for such attack vectors. A malicious Web site that you visited may attempt to exploit vulnerability in your Web browser. A firewall and anti-virus software help combat this threat, but keeping up with applications and OS patches provides another highly effective layer of protection. Not relying on a single security mechanism to protect you against attacks is the fundamental principle of Defense in-Depth (43).

Why should I be concerned with computer security? I am not a big company with millions and billions to steal.

Anyone who has a computer and shares information, whether it is through the internet, email, or floppy disk, has a responsibility to the computer user community as a whole. For example, a virus that gets emailed to us can use our address books to infect others. Or, our computers could be used without our knowledge to store illegal software or images. We must all balance the risks associated with the ease of information transfer.

There are three major principles of security: confidentiality, integrity, and availability. You want the documents on your computer, the emails you send & receive, and the credit card information you type in to purchase gifts over the Internet to be confidential. You do not want just anyone knowing this information. Similarly, you do not want the resume you post on hotjobs.com to be altered or the prices of the flowers you are sending to change when you go to checkout. This is integrity. Lastly, you want this information available to be read/written by you anytime or to be shared with your friends or organizations. (Cert 9/17/03; Cole, Fossen, Northcutt, Pomeranz 295-6). So, in other words, you want to make sure your information stays private; it isn't changed or altered without your permission; and you or anyone you deem acceptable can access this information anytime.

Risks can come from just about anywhere. The email your grandmother sent you could contain a virus. The web site you are perusing runs a cute animation that, known or unknown to the host of the website, is a cover for a Trojan horse being installed on your computer at this moment. They can be from non-computer-centric things like blowing a fuse and then the subsequent power surge on the return of electricity fries your computer. Or, as my sister just discovered, anything with moving parts can just break, including computer hard drives. Lastly, the risk can come from you. As I will explain later, by not securing

your computer, you may be inadvertently playing a role in the spread of a worm, a defacing of a website, or acting as a repository of photos for a porno website or illegal software (Osterman 8/12/03).

At first, this may sound overwhelming but it is not. In our daily lives, we negotiate risks all the time. For example, when we cross the street, we are deciding/predicting if the car coming at us will stop at the crosswalk or not. That “negotiation” is called the risk model in the security environment. $\text{Risk} = \text{Threat (the car)} \times \text{Vulnerability (the chance the car will not stop)} \times \text{Impact (how badly you would be hurt)}$. (Cole, Fossen, Northcutt, Pomeranz 303-4, 306). Unconsciously, we solve this equation every time we step off the sidewalk. We determine if the risk of being hit by a car is too great or a slim chance. For example, walking in front of a car moving 40 mph is a high risk, so we just glare at the driver from the safety of the sidewalk. In contrast, walking in front of a car, which is already stopped, is a low risk, so we will cross the street. The same principles apply when you connect to the internet. The risk of intrusion will always be there because the threats never disappearing. However, the level of risk is in your hands. You can control your vulnerability and your impact if something does happen.

7 Steps to Protecting your Computer by Reducing your Vulnerabilities and Impacts

1. Installing and updating an Anti-Virus Program
2. Installing an anti-spyware/adware program
3. Installing a personal firewall
4. “Locking down” or Hardening your Windows system
5. Updating your Operating System: Windows, Mac, Linux
6. Surfing Safer
7. Backing up important files

Note: To avoid bogging down the readers in definitions, I have added just the key terms for a step at the beginning of its respective section. A more thorough glossary of computer security terminology is located at end of the paper.

Anti-Virus Programs

Key Anti-Virus Terminology:

Trojans

Trojan Horses or Trojans are malicious programs that masquerade as helpful applications. Once installed, they collect and transmit information about you. Hackers and identity thieves use Trojans to steal login names,

passwords, and credit card information. A popular method of transmitting Trojans is to disguise them as a "music file" on an Internet site, waiting for someone to download and activate it. They are also frequently disguised as an update to Windows, or even as an update to anti-virus software. Many defense measures, such as anti-virus programs and firewalls, do not detect Trojans. (Webroot, 10/1/03)

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems (Webopedia, 10/1/03)

Worm

"A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively" (Cole, Fossen, Northcutt, Pomeranz A-148)

Zombie

Computers that contain software that allows an outsider to take over the machine for illicit activities. For example, in a Denial of Service attack, the zombie machines are called by their master to do their masters' (hackers) bidding. (Cole, Fossen, Northcutt, Pomeranz 634). The bidding can be set in the agent/program or be done through a broadcast on the internet. The owners of these zombie machines usually are unaware of their computers extracurricular activities

Why do you need anti-virus? Because any time you share information, you have a risk of contamination. Whether or not your computer is connected to the internet is immaterial. In the early 1990s, I spent a number of my working hours in the college computer labs clearing virus off of hard drives that were brought in via floppy disks.

How much damage could viruses or worms do? It depends. Some could produce a small nuisance like reordering your desktop, but others could take down thousands of machines worldwide. A virus or a worm could wipe out your

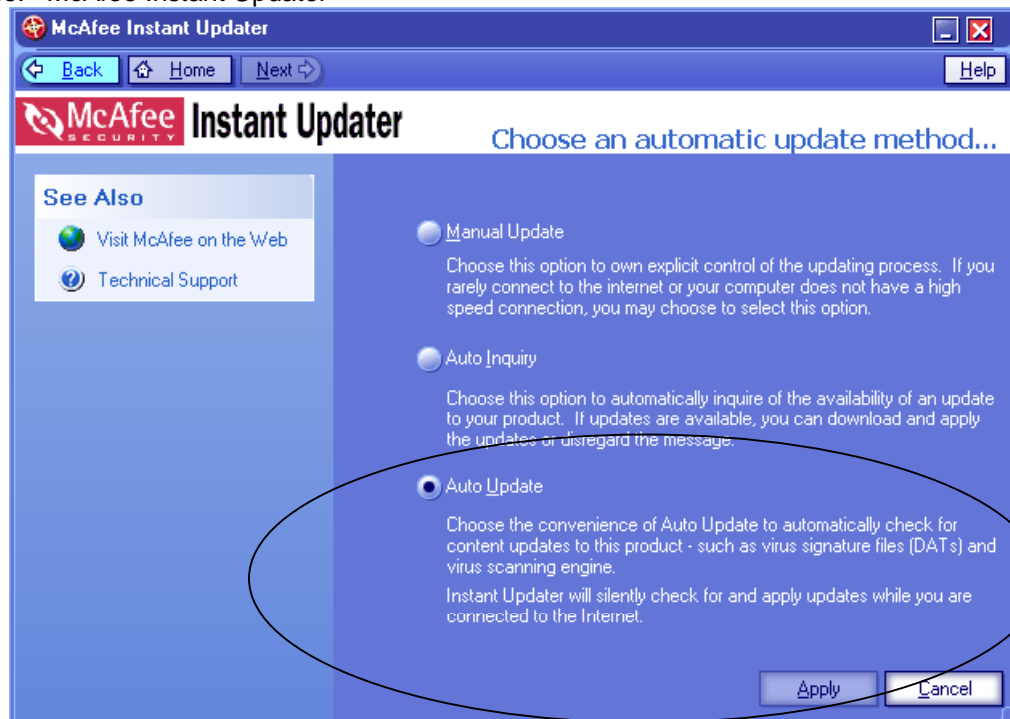
computer, open back doors for intruders to worm in through, steal files and then email them to others, clog up email servers with mass-emailings, or make your computer into a zombie (SANS, 9/15/03).

There are two important concepts to keep in mind about anti-virus software. One, you absolutely need to have one installed on your PC before an attack. While often there are ways to cure the virus after the attack, there are those virus/worms so destructive that the best solution is to wipe the hard drive clean (SANS, 9/15/03). This means erasing everything off of the computer including all programs and formatting the hard drive. Prevention is always a lot easier than diagnosing a virus/worm and cleaning up after the fact. So, spend the \$35.95 or so and purchase and/or renew your annual subscription. This leads me to step number two, keep your anti-virus program up to date. Anti-virus software companies could not stay afloat if the virus signatures from 4 years ago cured all of the viruses today. New viruses and worms are coming out weekly, if not daily. For each new virus type/pattern, a new signature is developed. Therefore by keeping your anti-virus current, you can greatly reduce the chance of being infected. One of the easiest ways to update your anti-virus software is to have the software update itself automatically.

This is also one of the safest ways to update your anti-virus. Invariably, hours after the nightly news broadcasts the newest destructive worm or virus, emails are sent out with spoofed or mocked email addresses. These emails provide links to "update" the reader's anti-virus program. Instead, these links really lure the reader to download Trojans or viruses. Or, these download sites are used for personal information/identity theft. The readers are told they need to purchase the updates so they enter their name, address, and credit card numbers. The moral is... always use the update feature within your anti-virus program.

Defense for the Home User: The Why & How

Example: McAfee Instant Updater



Anti-Spyware/Adware Programs

Key Anti-Spyware/Adware Terminology

Adware

Adware is software designed to track your buying and surfing habits, as well as demographic information and, sometimes, personal information. Sometimes classified as spyware, Adware may be installed on your computer when you install a shareware or freeware utility. Once an adware program is running on your system, it can track your activities and subsequently transmit reports to a remote computer for advertising purposes. (WebRoot, 10/1/03)

Back Door

A remote access & control program often installed via a Trojan. The term is based on the idea that even if you have the front door to your house padlocked shut, if the back door to your house is ajar, people and mosquitoes may come in without your knowledge. Moreover, these remote access/control programs are

like a thief possessing a set of keys to the back door. Intruders may unlock the door when they enter and lockup after they leave so no one else can get in.

Spyware

Spyware is loosely defined as any program that covertly gathers information through your Internet connection without your knowledge. Once installed, spyware programs monitor user activity on the Internet and transmit that information to interested parties.

In addition to wasting bandwidth, certain spyware programs can gather information about email addresses, keystrokes, cookies, and even passwords and credit card numbers. Many Spyware programs have been known to cause system failure and general system instability. (Webroot, 10/1/03)

Although a relative newcomer to the security medicine bag, anti-spyware programs are ever more common (Zone Lab 2). In fact, Earthlink.net has just added its derivative of WebRoot's Spysweeper, called SpyBlocker, to its set of tools ("Updated News", Webroot, 10/1/03). Why would Earthlink.net do this? Because between year 2000 and 2003, the number of Trojans and spyware detected worldwide on the internet has nearly doubled (Zone Lab 2). If you have ever had your homepage change without your knowledge or fought a series of popup windows that cannot be stopped until you totally exited out of Internet Explorer or Netscape, then you have been a victim. Usually though, there are no overt signs that you have been infiltrated.

Anti-spyware programs focus on three types of intrusions: spyware, adware, and Trojans. Although similar in concept as a virus or worm, these are three things that, currently, anti-virus software deals with little or not at all (Zone Alarm 2). Therefore, other companies have filled the void. Two common anti-spyware programs are Webroot's SpySweeper (<http://www.webroot.com/wb/products/spysweeper>) and LavaSoft's Ad-Aware (<http://download.com.com/3000-2144-10045910.html>). I have used both and have no preference. In general, anti-spyware programs work similarly to anti-virus software. You install the program on your computer. On a scheduled basis, anti-spyware will scan your computer for new intrusions and either delete or quarantine whatever it finds. Periodically, the anti-spyware will need to download new signatures to tackle new spyware that has been detected on the internet. So, just like with anti-virus software, you should set up your anti-spyware software to automatically download/update.

How do I get spyware/adware? "Typically, it is unclear who is responsible for deploying the spyware or what they do with your information once it is

collected” (Zone Lab, p. 2). However, we have a better idea as to how. Generally, they are downloads you are not aware are happening or realize you are downloading but didn’t mean to (like from a banner advertisements). The streaming audio and video files that play in QuickTime, Real Player, or Windows Media Player is another way to download it. How? Often to help the performance, you download part or the whole song/video. Tucked in the download, next to media file could be a Trojan.

Here is an example of a recent scan:

Example: Results of a Spy Sweeper scan



Personal Firewall

Key Firewall Terminology

Firewall: A hardware device or software on a computer used to prevent unauthorized access to computer files, folders, or resources.

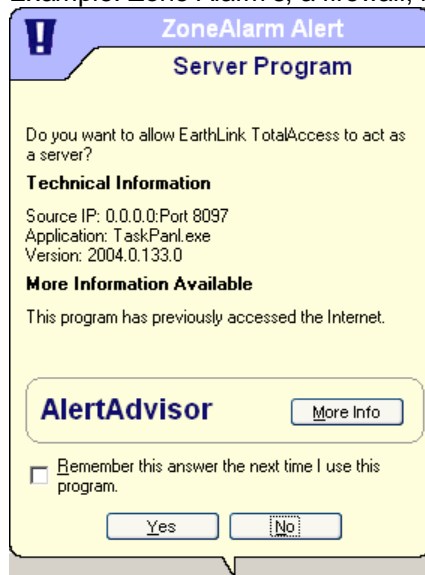
While the need for personal firewalls (software based firewalls installed on the computer) has always existed, it is with the advent of home users using broadband connection that put firewall in the forefront. When you connect to the internet, your ISP gives you a unique address. When you use a dial-up modem, you connect, do what you need to do online and then disconnect. Each time you dial-in, you are getting a new address. This makes it difficult to hack into your computer. You are literally a moving target. In contrast, broadband connections are rarely disconnected. As such, broadband is often referred to as “always on” (Microsoft, “Security & Privacy for Home Users” 9/17/03). Because the connection is rarely renewed, your IP address rarely changes. If you are hosting a website, your ISP may have given you a “static” address which means it will never change. In addition, many ISP dedicate a set of IP address just for home users (Cert, 9/17/03). This is like having the zip code 90210. Intruders can focus on the home users betting on the fact that many people fail to protect their

computers. Lastly, if you use a cable modem, there is an additional risk of intrusion because you are really just sharing the cable “pipe”. Anyone along the pipe can potentially get into your computer (Microsoft, “Security & Privacy for Home Users” 9/17/03).

One of the best ways to protect your computers is to install a personal firewall. There are many on the market, such as McAfee, Norton, Zone Alarm, Tiny Personal Firewall, as well as the Internet Connection Firewall that comes default within Windows XP. Except for the Internet Connection Firewall that comes with XP, all of these firewalls are called application control firewalls. They filter out traffic not pertaining to your computer, as well as create a specific set of access rules for the software installed on your computer (Cole, Fossen, Northcutt, Pomeranz 671). By answering the questions that pop up when you try to move around the internet, you train the firewall to know when to reject an incoming or outgoing request and when to accept.

Below is a firewall training popup used by one of the application control firewalls, Zone Alarm. It is asking me if I want to allow my Earthlink software access to the internet. As this is how I always connect to the internet, I will click “Yes” and check the box “Remember this answer the next time I use this program” so that my firewall will not have to ask me again.

Example: Zone Alarm's, a firewall, learning pop-up



Why am I asked this question? Because firewalls work on the principle of “deny all except that which is explicitly allowed” (Cole, Fossen, Northcutt, Pomeranz 656). What I am doing above is “explicitly allowing” for Earthlink’s

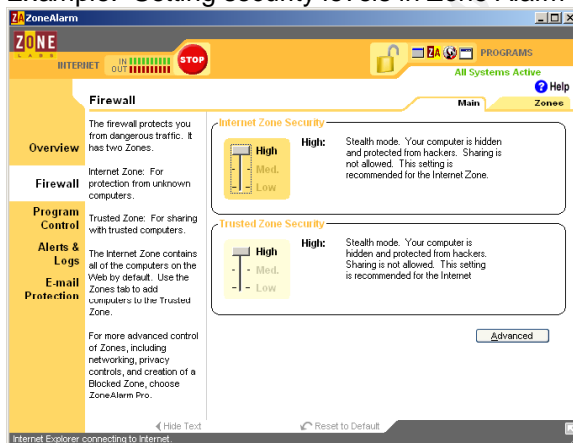
Defense for the Home User: The Why & How

TotalAccess to access the internet. Sometimes you may not be familiar with the programs requesting access to the internet. In these instances, it is better to say NO, uncheck “Remember this answer...” and then see what happens. If you were wrong and that application should have access to the internet, then simply close the application in question and say YES the next time your firewall asks. Remember what your mother said, “It is better to be safe than sorry”.

How safe you want or can be depends what you need to do online.

Therefore, there are scales in how strict a firewall can or will be. For example, Window’s XP Internet Connection Firewall will by default block any traffic not directly invited in by the user. When you check for new email, you are permitting the firewall to open a door (called a port) to the internet and only to send/receive emails. As soon as the emails have been sent and been received, the door closes until the next query for new emails. This is very secure. But, it will be too severe for those wanting to do online gaming or to host a web server. If users want to do these activities, they must manually open specific ports to allow the desired traffic to come in –i.e. prop open some doors in order to let the gaming/file sharing traffic through (Microsoft, “Frequently Asked Questions About Internet Firewalls 9/17/03). In Zone Alarm, the user raises or lowers the level of protection by dragging the level up and down, from High to Low. As with other firewalls, each level has a description to help you determine the how secure you can be without inhibiting on your work.

Example: Setting security levels in Zone Alarm



Internet Connection Firewall

As I mentioned earlier, the firewall that comes default with XP, Internet Connection Firewall (ICF), works differently than Zone Alarm and many other personal firewalls. According to Microsoft’s Help files,

ICF is considered a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communications that cross its path and inspects the source and destination address of each message that it handles. To prevent unsolicited traffic from the public side of the connection from entering the private side, ICF keeps a table of all communications that have originated from the ICF computer ("Internet Connection Firewall Overview" 9/17/03).

This means if I request a web page from www.amazon.com, only a web page from www.amazon.com will be allowed to go through the firewall. If my Quicken program asks for the newest download of my credit card information, ICF will allow a download from my credit card company because the request originated from my computer. In other words, unlike the application control firewalls, ICF does not need user interaction because it assumes whatever your computer asks for is authorized. This works well but it does have one fallacy. Just because a request originates from your computer, it does not mean it is "good."

When the MS Blaster worm first came out, there were no virus signatures for it yet. So, the anti-virus programs could not kill it, yet. Once it got on to a computer, it used your computer to look for other computers who had DCOM enabled (a vulnerability in Microsoft). Because this infestation call originated from the computer, the Internet Connection Firewall did not stop it. The firewall just assumed the traffic going out was legitimate. If the firewall had egress (outbound) filtering, then the computer owner would have a way to stop the Trojan from spreading from his/her computer. Or, in the case of application control firewalls, the computer user would have had a choice to allow this traffic out or not.

How to setup the default firewall in Windows XP -- Internet Connection Firewall.

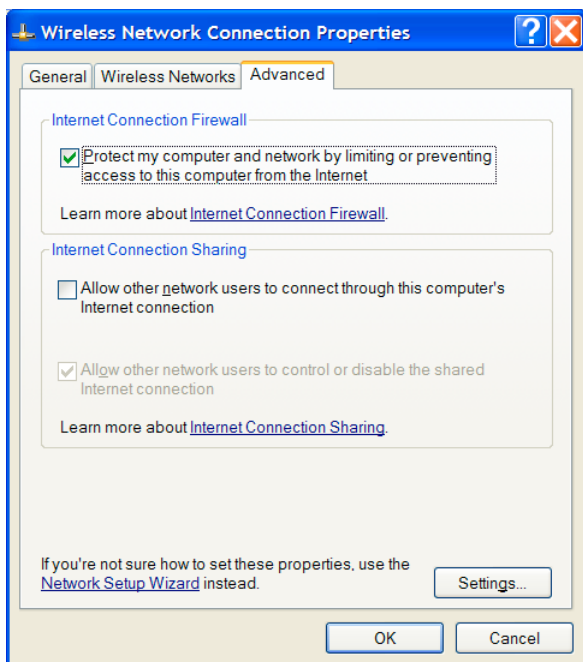
1. Go to Start Menu
2. Go to "Connect To" (If you do not see your connection, select Show All Connections)
3. Double-click on your internet connection (LAN or modem).
4. Go to the tab called "Advanced"

If the connection is wireless you will this:

Example: Wireless Network Connection Properties ICF

(Note: XP Home Edition does not have the Internet Connection Sharing panel.)

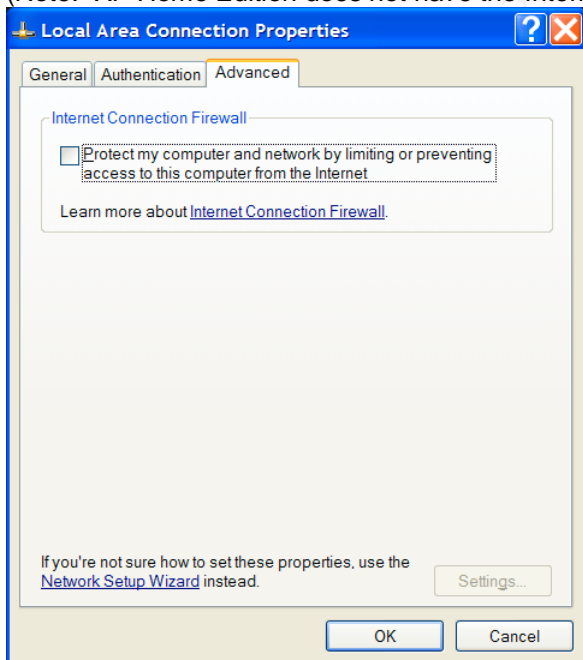
Defense for the Home User: The Why & How



If your connect is not wireless, you will see this:

Example: Local Area Network Connection Properties ICF

(Note: XP Home Edition does not have the Internet Connection Sharing panel)



Logging:

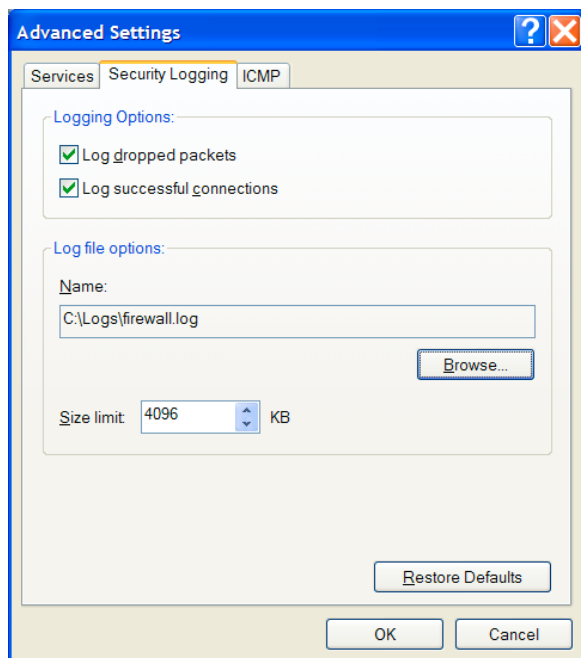
In addition to enabling a firewall, you should turn on logging to help troubleshoot future problems. I am not just talking just about intruders. While logs are good way to see if your computer is acting as a zombie or if you have a worm trying to spread, you will more likely use it to determine why something is not working. As I mentioned earlier, the default settings for ICF block you from participating in online games or using AOL dial-up (Microsoft, "Frequently Asked Questions About Internet Firewalls" 9/30/03). If you looked at the log, you would see that ICF was blocking these activities and you could take steps to mitigate this.

How to Setup Logging

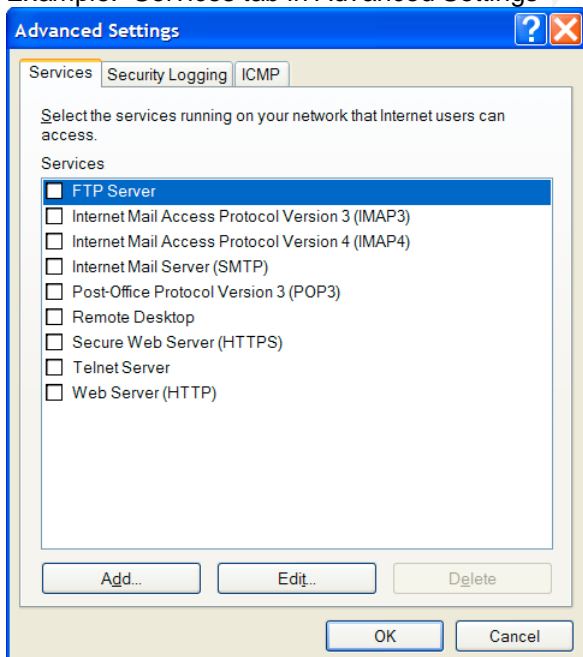
1. To enable logging you need to first enable the firewall. When you do so, the "Settings" button will become active (un-gray).
2. Click on this "Settings" button. This will take you to the "Advanced Settings" window.
3. Go to the second tab "Security Logging".
4. Select both "Log dropped packets" and "Log successful connections".
5. You should probably change the default location of the log file, too. If an intruder wanted to alter your log to cover his/her tracks, it will be harder to find if it is not in the default location.

Example: Enabling Security Logging in ICF

Defense for the Home User: The Why & How



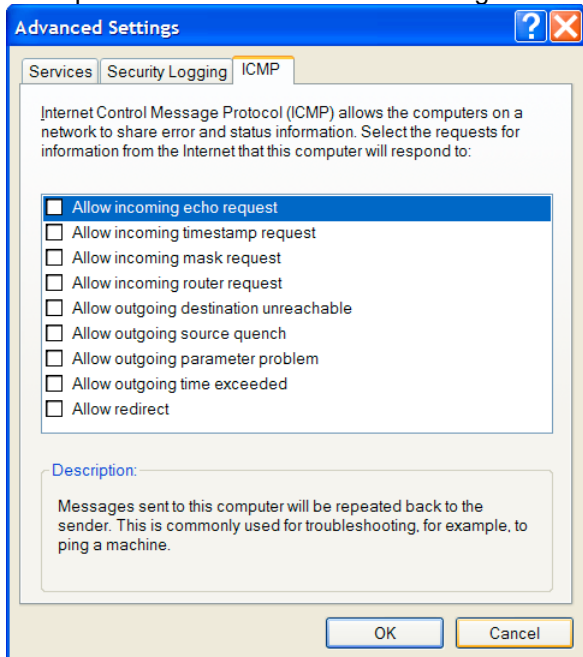
Other settings in Advanced Settings:
Example: Services tab in Advanced Settings



The example above shows the services available, but automatically disabled. These should only be manually enabled if you are planning on hosting a web site (HTTP or HTTPS), FTP server, or Email Server (IMAP3, IMAP4, SMTP, POP3). If you would like outsiders to connect to your computer, you may want to check Remote Desktop or Telnet Server. However, I **STRONGLY** recommend that you do not manually check anything. Each service enabled makes you that much more vulnerable to attack.

The last tab in Advanced Settings, "ICMP," should not be touched. I cannot think of a reason why a regular home user would want or need to have any of these activated.

Example: ICMP tab in Advanced Settings



HARDENING YOUR COMPUTER

Depending on your computer skills, there are a number of different things you can do to "harden" your computer. When you harden your computer, you are trying to reduce your vulnerabilities to intruders by eliminating some of the possible doors for them to walk through.

Creating A Local and An Administrator Account

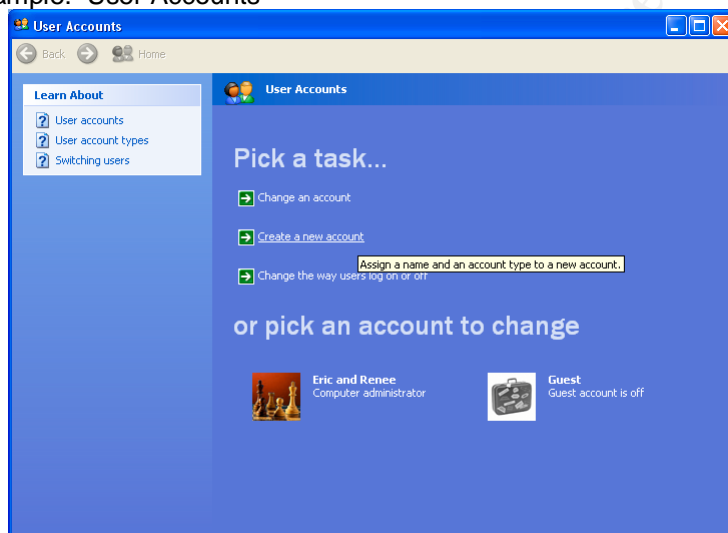
Unfortunately, when Microsoft puts out a new operating system for the home users, they weaken some aspects of their security settings. For instance,

XP for Home and Windows 98 make all users an administrator by default. This means each user can install, delete, and modify anything. This is dangerous, even for security and Windows experts. Therefore, I recommend having two accounts on the computer: one "limited user" and one "administrator". For most of the day-to-day things you do, the rights associated with "limited user" are sufficient. When they are not, for example if you want to install the newest version of Doom, then you can "switch user" and login as an administrator. This may also reduce the amount of spyware and Trojans that can be installed on your computer because many of these scripts and programs require more rights/permissions than those granted to the "limited user."

How to Create a Limited User account

1. Go to Start Menu and select Control Panel
2. Select Users Accounts

Example: User Accounts



3. Click on "Create a new account"
4. Next, type in the name of the local user
5. Select "Limited User"
6. Remember to add a password.

Passwords

Try not to have an easily guessable password—for Windows, for the website you use for shopping, for the credit card data download page, etc. The following are based on the recommendations of Cole, Fossen, Northcutt, and Pomeranz. All passwords should be 8 or more characters long. In fact, the

longer the password the better as each additional character makes it exponentially harder to crack. They should also contain at least one number and one character. In addition, try to use mixed cases (upper case, lower case) and do not use a derivative of your previous passwords. Lastly, and most importantly, avoid using names, words, or family birthdays. What should you use? Try modifying a phrase—e.g. Santa Claus is Coming to Town can be converted to S@C!lc02t0 or SntCl\$!sCmng2Twn (Cole, Fossen, Northcutt, Pomeranz 415).

Hidden File Extensions

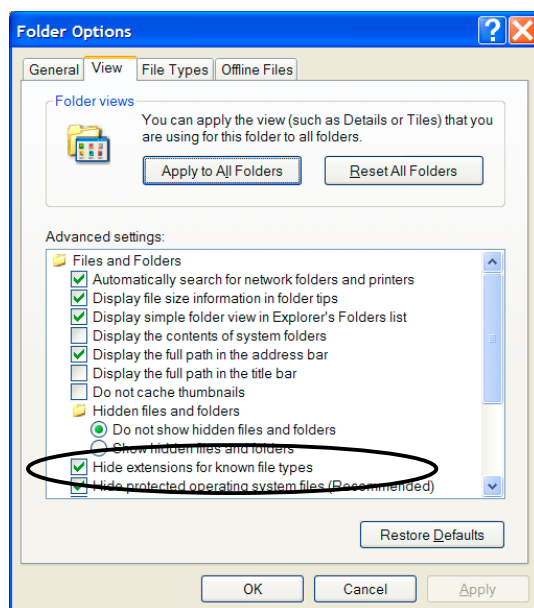
One of the reasons the LoveLetter virus spread so well is that it worked against one of Microsoft's "improvements" starting in Windows 2000 and Millennium. In order to make folders look cleaner, Microsoft decided to create a default setting to hide file extensions. [File extensions are the .doc, .xls, .jpg, .mpeg, and so on found at the end of a filename]. This virus and its relatives spread via emails with attachments. Knowing that most people have been told to be cautious of email attachments, the virus's creators disguised their virus script. In the case of the LoveLetter virus, they labeled the attachment as "LOVE-LETTER-FOR-YOU.txt.vbs" (Cert 9/17/03). If email recipients had seen the file extensions, less people would have double-clicked or opened the attachment. Why? Because (1) in Windows, files only have one extension and (2) the last file extension, .vbs, indicates the file is a script, an executable of sorts. Scripts, macros, batch files and executables DO things. If you are thinking you are just reading a love letter, you do not want or expect anything DOing something to your computer. Fortunately, most email programs now block these file extension. However, you should know a few file extensions to avoid when they are part of an email attachment's or a file's name on a floppy disk/CD. They are cmd, exe, bat, pif, and vbs.

How to show (un-hide) extensions for known file types

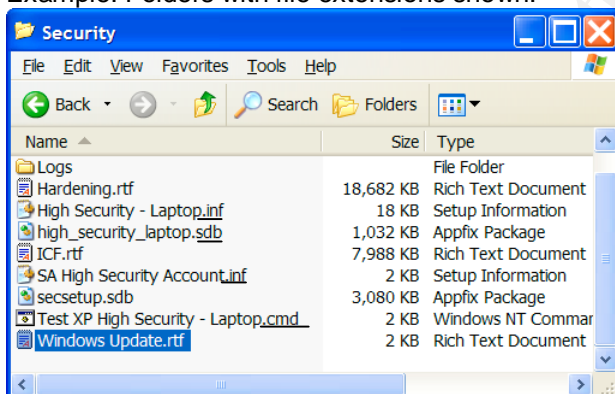
1. Double-click on My Computer
2. Go to the Tools menu and select "Folder Options"
3. Un-check "Hide extensions for known file types"

Example: View tab in Folder Options

Defense for the Home User: The Why & How



Example: Folders with file extensions shown:



Are you networking your computers at home? If not, here are some things you can disable.

Disable Server Message Blocks and RPC & NetBios over TCP/IP

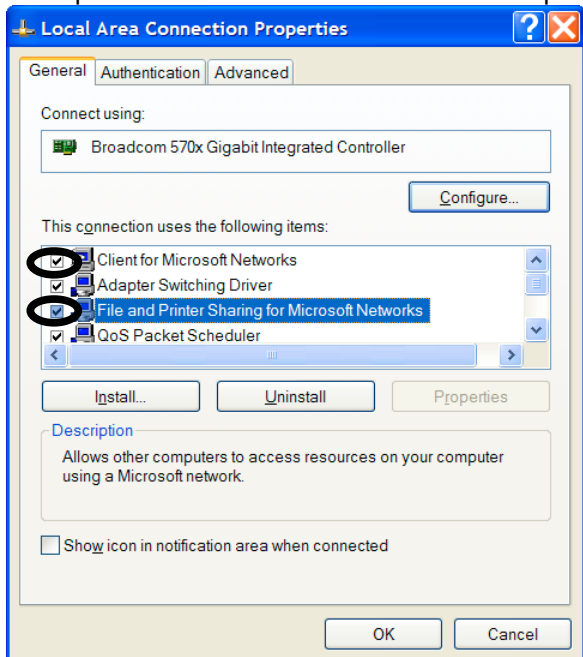
1. Go to Start Menu
 - a. XP only: Click on "Connect to" and select your dial-up or local area connection.
 - b. Windows 98/2000: Go to Control Panel and select "Dialup and

Defense for the Home User: The Why & How

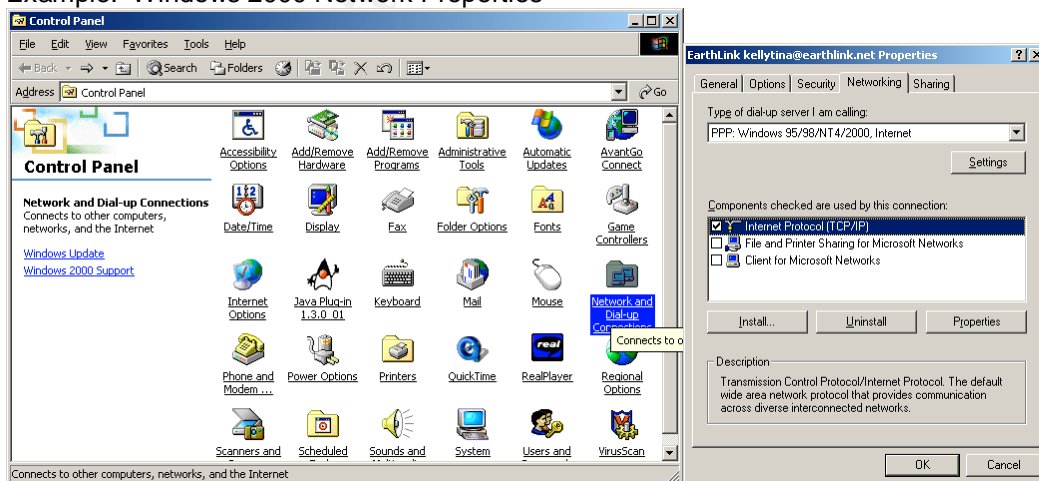
Network Connections".

2. Right-click on your mouse (click the right-hand button on your mouse) and select "Properties"
3. Uncheck "Client for Microsoft Networks" and "File and Printer Sharing for Microsoft Networks"


Example: Default Local Area Connection Properties settings



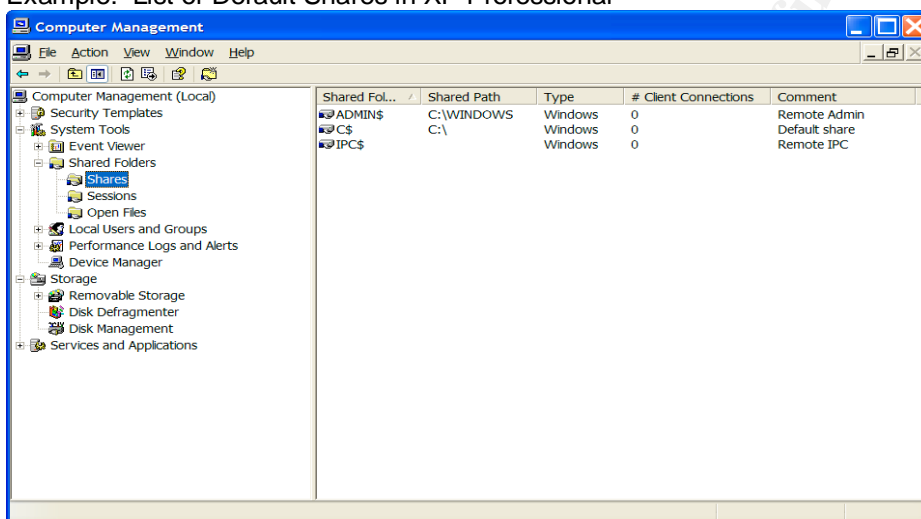
Example: Windows 2000 Network Properties



Removing any unprotected shares

For reasons I do not understand, Microsoft creates default network shares. This means anyone on your network (or internet) can access these folders and drives--- if they have administrator rights (Microsoft, "Help and Support: Using Shared Folders"). In addition, one can manually create their own file/folder shares by first right-clicking on the mouse & then selecting "Sharing" or "Properties" and "Security". So, how do you know if you have any shared folders or files? Look for the arm/hand holding the folder, drive, or file: 

Example: List of Default Shares in XP Professional

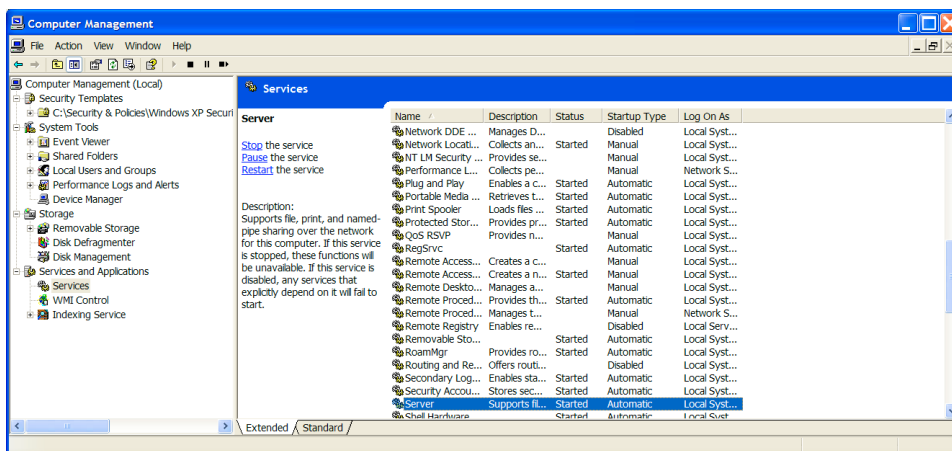


To remove the default shares, you have to stop the computer from acting as a "server".

1. Go to Start Menu
2. Go to All Programs and then Administrative Tools
3. Select "Computer Management"
4. Click on "Services and Applications"
5. Click on "Services" and find "Server"

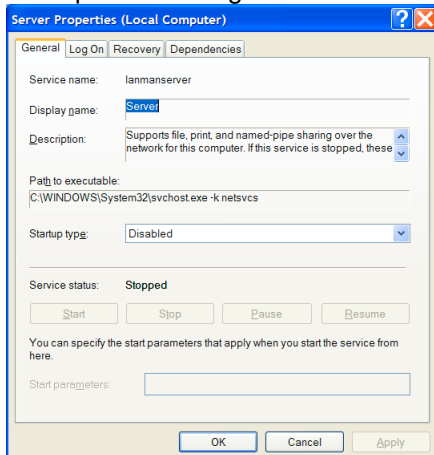
Example: Services in Computer Management

Defense for the Home User: The Why & How



6. Right click on "Server" and select "Properties"
7. In "Startup Type" and select "Disabled"

Example: Disabling the Service Server



Disable Remote Assistance/Desktop

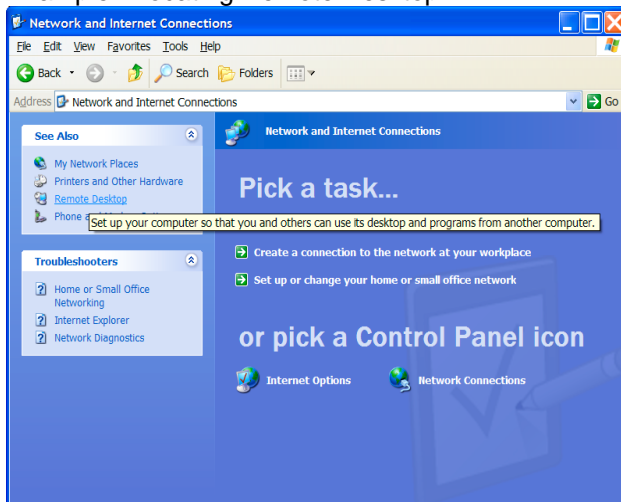
XP comes with a feature that allows people to control your computer from the internet or a home network. As you may imagine, this is not something you want to make available all of the time. But, it could be useful if you need help from outside. For example, I can imagine connecting to my mother's computer to teach her how to burn a CD or to help troubleshoot why her scanner is not working. But, for the 99.9% of the time, she should uncheck both "Allow Remote Assistance invitations to be sent from this computer" and "Allow users to connect remotely to this computer".

Defense for the Home User: The Why & How

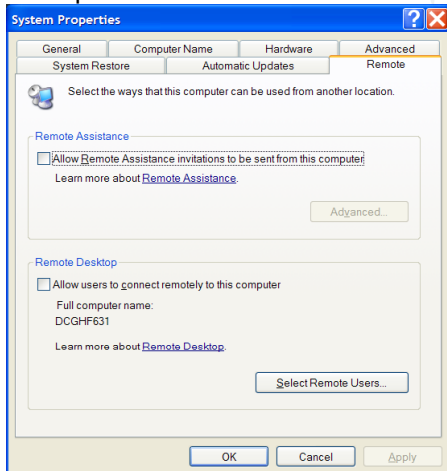
How to Disable Remote Assistance & Remote Desktop

1. Go to the Start Menu.
2. Click on Control Panel.
3. Click on "Network and Internet Connections".
4. On the left pane, you might see "Remote Desktop". If you do not, click on "See Also" and find "Remote Desktop".

Example: Locating Remote Desktop



Example: Where to turn on/off Remote Desktop and Assistance



Re-ordering the boot order in your Bios

When your computer first starts up, you will be given an option to go into

the Bios. Unfortunately the keys you need to type have not been standardized. However, in my experience, you usually click the Esc key, F12 key, or the F2 key. Once you are in the Bios, look for the screen that handles boot order. Using the Up/Down keys OR page up/ page down (again, this is not standardized), change the boot order so that your "C" drive is first in the order.

Securing Internet Explorer

According to SANS, if an intruder wants to exploit vulnerabilities within Internet Explorer, they usually use Java applets, Active scripting and ActiveX Controls ("SANS Top Twenty Vulnerabilities..." 10/14/03). Simply disabling these options is not the answer, though. Many of today's websites use these options to make some of their features work, including some anti-virus update programs. So, a "happy medium" must be found that does not hamper your ability to surf the web but limits an intruder's exploitation abilities.

SANS recommends:

1. "Select Internet Options under the Tools menu
2. Select the Security tab and then click Custom Level for the Internet Zone...
3. Under Scripting, select Prompt for Allow paste operations via script to prevent content from being exposed from your clipboard ...
4. Select Prompt for Download signed ActiveX Controls
5. Select Disable for Download unsigned ActiveX Controls
6. Also select Disable for Initialize and script ActiveX Controls not marked as safe....
7. Under Microsoft VM, select High safety for Java permissions in order to properly sandbox [contain] the Java applet and prevent privileged access to your system.
8. Under Miscellaneous select Disable for Access to data sources across domains to avoid Cross-site scripting attacks " ("SANS Top 20 Vulnerabilities..." 10/14/03).

Disabling Windows Scripting Host

Another one of Microsoft "improvements" starting with Windows 98 is a technology called Windows Scripting Host (WSH). Because WSH gives scripts access to the meat & bones of the operating system (e.g. the shell, file system, registry), scripts can now be run directly from the desktop or through programs, like Outlook and Word ("SANS Top Twenty Vulnerabilities" 10/14/03). This is great for automation as it works no matter if the user is "administrator" or "limited

user". Regrettably, because it works so well, WSH has been a great asset for virus writers like the one(s) who created "The Love Bug" or "ILOVEYOU" viruses ("SANS Top Twenty Vulnerabilities" 10/14/03).

Fortunately, it is generally unnecessary to have this "improvement" enabled. Even better, if you have 2000, Millennium or XP, Symantec (an computer security company) has created a program called Noscript.exe that disables WSH for you ("SANS Top Twenty Vulnerabilities" 10/14/03). This same program can re-enable WSH, if for some reason you need it. Windows 98 users can use same web page to find the instructions on how to disable WSH on their computer (Symantec. 10/15/03).

How to Disable WSH

1. Go to www.symantec.com/avcenter/venc/data/win.script.hosting.html#removalinstructions and find the download for Noscript.exe
2. Download the Noscript.exe and save it in the "Download" folder you previously created
3. Double-click on Noscript.exe
4. When prompted click "Disable" and then OK (if you have to re-enable WSH, click "Enable" instead)

Outlook and Outlook Express

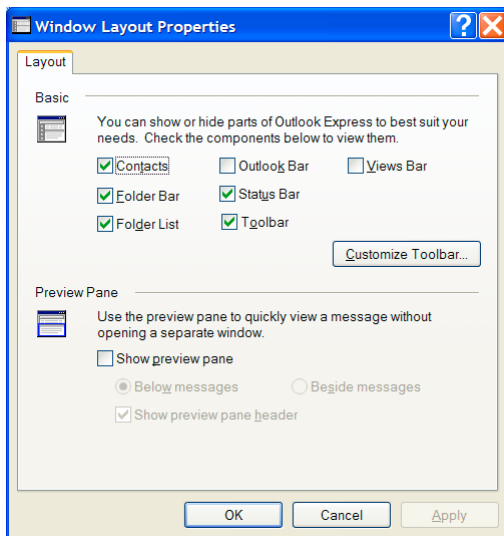
Because Outlook Express comes default with Internet Explorer and Outlook is usually installed as a part of Microsoft Office, there is a good chance you may be using one of them. Like many of Microsoft products, they need to be hardened. SANS recommends disabling the Message Preview pane and restricting email site zones ("SANS Top Twenty Vulnerabilities..." 10/14/03).

To avoid "reading" a virus-infected email, disable the Message Preview Pane.

1. Open either program
2. Click on "View" and go to "Layout"
3. Un-check "Show preview pane"

Example: Unchecked "Show preview pane" in Window Layout Properties

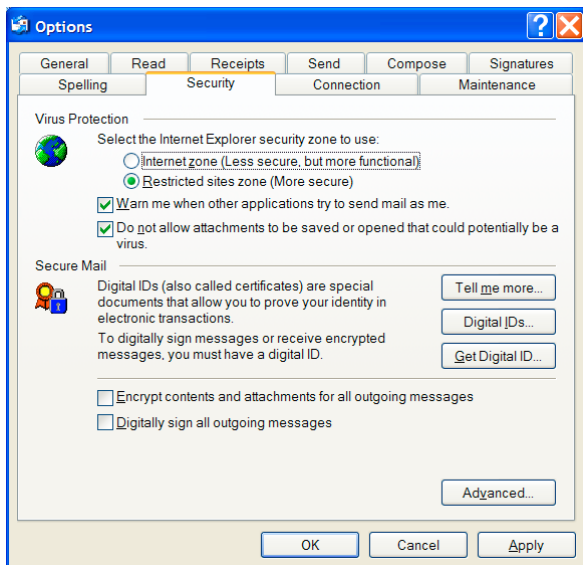
Defense for the Home User: The Why & How



Activate the security options available in Outlook/Outlook Express

1. Go to the "Tools" menu and select "Options"
2. Click on the "Security" tab
3. Check "Restricted sites zone (More Secure)"
4. Outlook Express Only: Check "Warn me when other applications try to send mail as me". This is to avoid email-spoofing
5. Outlook Express Only: Check "Do not allow attachments to be saved or opened that could be potentially be a virus". This feature can block legitimate attachments too.
6. If you get an email with an attachment blocked by Outlook/Outlook Express that you feel to be safe, uncheck this option.
7. Save the attachment to your "Download" folder and scan it for viruses.
8. If it came back, virus free then open it up. You are most likely safe and a risk I usually accept.

Example: Security tab within Outlook Express



Updating your Operating System

It is important to keep your computer up-to-date. This is especially true if you are using Microsoft software or operating systems (ex. windows 98, 2000, XP). What about Apple? Well, while there have been security problems with the Mac OS, they tend to be rare. I think the reason is that proportionally fewer people have Macs so fewer people are looking for holes. Therefore, if a hacker, especially script kiddies, wants to break into the greatest number of computers as possible, so they will stick with the Microsoft and Linux varieties. However, this doesn't mean all hackers. Therefore, use the same defense in-Depth principles no matter what operating system you are using.

How can I keep my Windows system up-to-date?

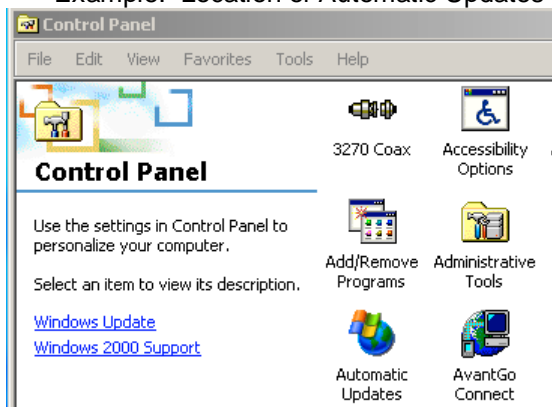
First, a warning: Just as with your anti-virus programs, only update Windows through its Automatic Updates program. Why? One of the most recent viruses, Swen, spread through fake/spoofed emails from Microsoft warning the reader they needed to update. When the reader clicked on the "update" link, they got a virus instead (Cert 9/17/03).

Configuring Automatic Updates

1. In XP (and Windows 2000 sp3 or greater), setting up automatic updates is easy.
2. Login as an administrator
3. In Windows 2000, go to the Start Menu and select Control Panel.

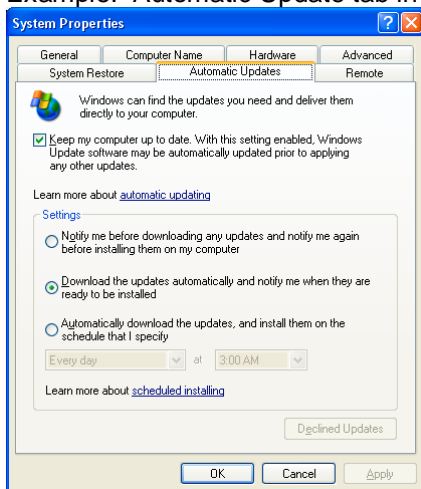
Defense for the Home User: The Why & How

Example: Location of Automatic Updates in Windows 2000



4. In Windows XP, go to the Start Menu and select Control Panel. Click on Performance and Maintenance (if it is not visible, then click "Switch to Category View"). Click on "System"

Example: Automatic Update tab in XP



5. On the "Automatic Updates" tab, check "Keep my computer up to date"
6. Select your settings. I recommend "Download the updates automatically and notify me when they are ready to be installed". Microsoft recommends the last option of "Automatically download..." (Microsoft "Protect Your PC: Print All Three Steps" 9/17/03).

From time to time, you will now notice the Automatic Update icon appearing in the taskbar to the right and saying you have updates from Microsoft available. I recommend installing them one at a time. This way if something stopped working, it will be easier to determine what caused the problem. And if you are using XP, you can rollback to the last working version.

You can use this rollback feature anytime your computer begins to crash or have a lot of problems.

1. Go to Start Menu
2. Go to Control Panel
3. Go to Performance and Maintenance
4. On the upper left pane, you should see the option called "System Restore"

Verifying that your computer is up to date

Periodically, test your computer for vulnerabilities. One way to do this is to run <http://www.sans20.qualys.com/>. Once you have filled in a form, you will be asked to download an executable. Save this file on your computer. [I always create a folder called "Downloads" or "My Downloads" and everything I download to this folder.] When you run this program, it will compare the settings on your computer with the top 20 security vulnerabilities. It then gives you suggestions on how to fix some of the issues. Microsoft has a similar product called Microsoft Baseline Security Analyzer. You can download it at <http://www.microsoft.com/downloads/details.aspx?FamilyID=9a88e63b-92e3-4f97-80e7-8bc9ff836742&DisplayLang=en>.

Surfing the Web and Emailing Safer

I am not going to delve deeply in this section because most of it is common sense. For example, do not believe everything you read. If you get an email saying you won a lottery and you didn't play that lottery, erase the email. If you receive an email with a subject line that makes no sense, especially if it came from an email address you do not recognize, delete it (see the example below). In other words, just as you get junk mail in your mailbox, you will get spam (junk email) in your email mailbox. If you feel you are getting too much spam, there are spam blockers that you can purchase. In addition ISPs, like Earthlink, are now providing a spam blocker for free to their users.

Example: Spam

From	Subject	Received
 guney sieczko	hyu big bat = home runh	10/7/2003 12:06 A...

Be wary of pop up messages claiming everything under the sun— to secure your PC for only \$20 a month, to sell video camera for only \$9.99, to giving you \$100 if you participate in a survey, and so on. In addition, whenever possible use the ☒ on the upper right-hand side of a window to close the window rather than the "Close" button. In essence, there is code behind every button that defines what a button will do. Most of the time, the code behind a "Close" or

Page 28 of 38

Submitted On: 12/5/2003

“Exit” button does exactly that, closes the window or exits the window, respectively. However, there is no way for you to do for certain what the code behind a button really says to do. This is especially true with popup messages as their goal is to lure you somewhere. Like with spam, there are popup blockers you can purchase or download or coming automatically with you ISP. I use “Stopzilla”, www.stopzilla.com, and find it blocks every pop up I do not want but gives me the freedom to allow the ones I need – like the calendar for expedia.com.

Instant Messaging (IM), chat rooms, and newsgroups are good ways to meet other people and to pick up viruses and Trojans. So, do not accept files from strangers. Be cautious about how much personal information you want to devolve. Pornography newsgroups and chat rooms are renown for being the first places worms show up. So, determine how much risk you are willing to accept before downloading anything from pornography sites—or any other newsgroup, chat room, or website.

Music, video, photograph, and proprietary software sharing through Kazaa, Gnutellas, eDonkey, and their relatives use a type of networking called peer-to-peer (P2P). The software allows the user to share files or folders, as well as to help index other’s collections. Besides the legal ramifications of swapping music and movies, there are some significant security risks. A poorly configured P2P could open the user’s computer to sharing just about any data file (“SANS Top 20 Vulnerabilities 10/14/03). In addition, spyware is often included with these P2P softwares. So, over and beyond the sharing of files, you are now sending out information on you where you go on the web. Lastly, be careful of what you download. Just because a file says “Madonna: Truth or Dare” doesn’t mean it is only a video file or a video file at all. Make sure the icon fits the file type and that the file has only one file extension (SANS. “SANS Top 20 ... 10/14/03)

Backup your data periodically

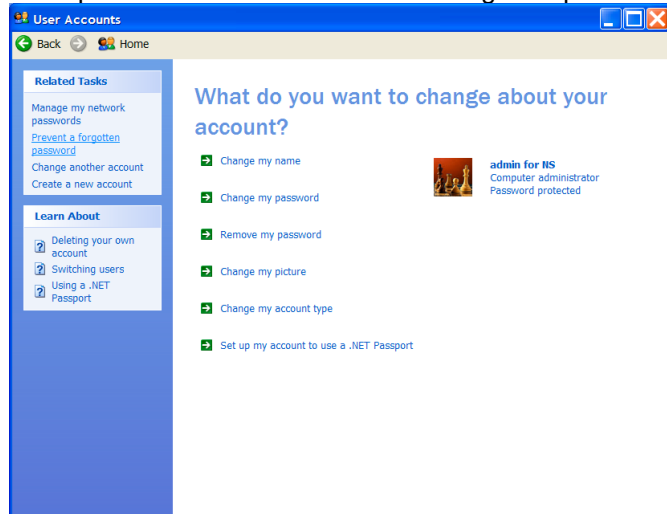
Backing up your Passwords

Starting with Windows XP, you can backup the passwords to your user account onto a removable media like a CD-Rom or a floppy. Now you should have no reason to use easily crack-able passwords, because now you can recover your password if you forget it.

1. Go to the Start Menu
2. Open Control Panel
3. Go to User Accounts

4. Click on "Protect a forgotten password"

Example: User Accounts—Protect a forgotten password



Backup of Data

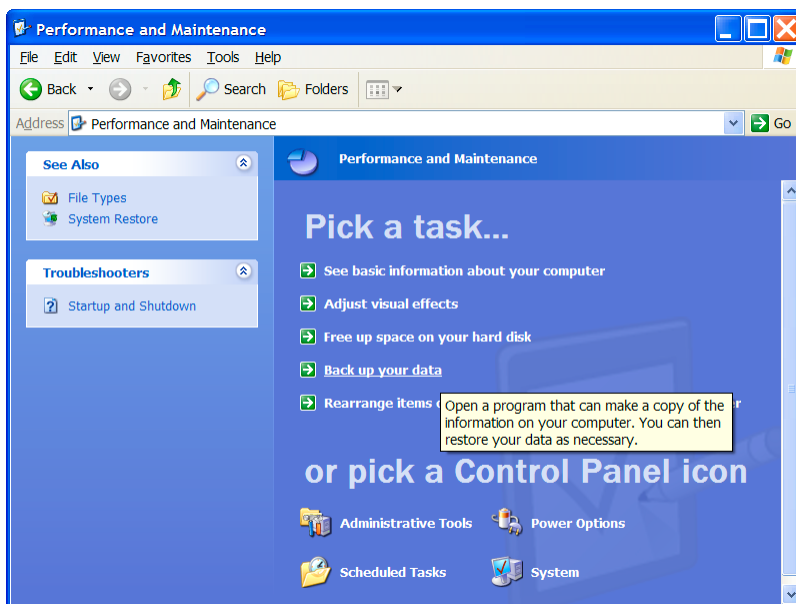
Two weeks ago, my sister's hard drive had a mechanical failure and stopped working. Unfortunately, she failed to backup any of her files. She has now permanently lost photos of her children, her bank registry in Quicken, her favorites in Internet Explorer, etc. If she had done a weekly or monthly backup, she would have been able to recover these items.

How to Backup Data: XP

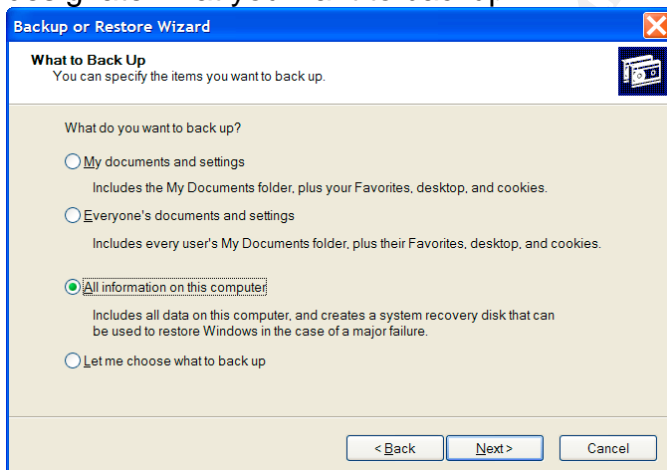
1. Go to Start Menu and open the Control Panel
2. Click on "Performance and Maintenance"
3. Select "Back up your Data"

Example: Selecting "Back up your data"

Defense for the Home User: The Why & How



A wizard will lead you through a series of questions. You will eventually have to designate what you want to backup:



There is no all-purpose answer as to what you should backup and how often. It depends on what you are doing and how often you are making changes. Simply, back up anything you do not want to lose. This means if you have just spent 18 hours creating on a killer presentation, take an additional 5 minutes to burn it on CD.

Suggestions: If all of your files are in the "My documents and settings" folder, then you could use option one weekly and "All information on this computer" monthly. This would not have helped my sister with her Quicken data so she would use the last option "Let me choose what to back up" and then

choose your Quicken data, as well as her "My documents and settings" folder. She would augment this back up with a monthly "All information on this computer."

Summary

Do I really need to do all of this?! Again, the focus of this paper is Defense in-Depth. The more layers of defense, the more secure you will be. Now that you know some of the risks, you can determine how much you are willing to accept. For me, the time it takes to harden my computer, setup my firewall, backing up my files, and keep up with the virus and spyware signatures is a wash compared to the time spent recovery from an attack or a hard drive failure. Lastly, home and business computer security is becoming an issue for the law. The risk of having an intruder install a back door and using my computer as a zombie or as a file repository is getting too high for anyone to ignore as people are now being arrested (The SANS. Vol5. number 42). So, put on your galoshes, raincoat, overalls, and umbrella and enjoy your connection to the worldwide web (www).

Lets end with a basic computer security glossary:

Adware

Adware is software designed to track your buying and surfing habits, as well as demographic information and, sometimes, personal information. Sometimes classified as spyware, Adware may be installed on your computer when you install a shareware or freeware utility. Once an adware program is running on your system, it can track your activities and subsequently transmit reports to a remote computer for advertising purposes. (WebRoot, 10/1/03)

Back Door

A remote access & control program often installed via a Trojan. The term is based on the idea that even if you have the front door to your house padlocked shut, if the back door to your house is ajar people and mosquitoes may come in without your knowledge. Moreover, these remote access/control programs are like a thief possessing a set of keys to the back door. Intruders may unlock the door when they enter and lockup after they leave so no one else can get in.

Cookies

"All they are is a simple bit of text which web sites use to identify a surfer in

some manner.” (<http://www.leave-me-alone.com/cookies.htm>. 10/1/03). Moreover, these bits contain only the information the surfers typed in themselves. For example, when I go to Amazon.com, my name appears on the treasure chest. How does Amazon.com know my name? Because last time I went to the site, I typed in my name to login to the site. Now my name is stored in a cookie on my local computer.

Does that mean my credit card information is stored in a cookie too? Possibly, but not likely. “In some rare instances, amateur webmasters actually store credit card or other sensitive data directly in a cookie. This is extremely bad practice ... Fortunately, it is fairly rare.” (<http://www.leave-me-alone.com/cookies.htm>., 10/1/03). This does not mean you should accept every cookie. If you do not recognize the source of the cookie, you can deny it. If you do indeed need the cookie to use the website, then close your web browser and go back to the site. This time accept the cookie in question.

Denial of Service (DDoS)

Attacks that cause a computer to crash or slow down to a point that it cannot do anything else. DDoS attacks are usually a result of a coordinated effort of multiple computers. A hacker will install an “agent”, like through a Trojan, on a bunch of computers. Then when the time is right, the hacker will call all of the “agents” into action to attack a particular computer or web server. (Cert, 9/17/03). These agent-containing computers are called “zombies” because when called by their master, they do their masters (hackers) bidding. (Cole, Fossen, Northcutt, Pomeranz 634). The bidding can be set in the agent/program or be done through a broadcast on the internet. The owners of these zombie machines usually are unaware of their computers extracurricular activities.

Email Spoofing

“Email ‘spoofing’ is when an email message appears to have originated from one source when it actually was sent from another source” (Cert. 9/17/03). For example, one of the most recent worms, Swen, was spread through an email appearing to come from Microsoft.com. Having a @Microsoft.com address “convinced” the email reader that the attached link to a patch was legit. (The SANS Institute 9/24/03)

Firewall

A hardware device or software on a computer used to prevent unauthorized access to computer files, folders, or resources.

Hotfix

A term almost solely used by Microsoft for its products, a hotfix is miniature program that fixes a flaw (bug) in the product

Internet

“A term to describe connecting multiple separate networks together” (Cole, Fossen, Northcutt Pomeranz A-135)

Network

A group of two or more computers linked together.

Patch

“A temporary fix to a program bug” (Webopedia “Patch” 10/1/03). A bug can mean a problem in a program that causes errors, stops things from working, or provides a means (a “hole”) for an intruder to enter a computer system.

Registry

A mini database that contains almost all of the settings for hardware, software, operating system, and user preferences (Cole, Fossen, Northcutt, Pomeranz 1206)

Script Kiddie

A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability. (Webopedia, “Script Kiddie” 10/10/03)

Service Packs

A cumulative set of patches and hot fixes.

Signature

A specific pattern of a virus, spyware, or attack. Diagnosing a pattern to an intrusion makes it possible to stop them by looking for incoming events that match this particular pattern.

Spam

Electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. However, if a long-lost brother finds your e-mail address and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. (Webopedia, "Spam" 10/1/03)

Spyware

Spyware is loosely defined as any program that covertly gathers information through your Internet connection without your knowledge. Once installed, spyware programs monitor user activity on the Internet and transmit that information to interested parties.

In addition to wasting bandwidth, certain spyware programs can gather information about email addresses, keystrokes, cookies, and even passwords and credit card numbers. Many Spyware programs have been known to cause system failure and general system instability. (Webroot, 10/1/03)

Trojans

Trojan Horses or Trojans are malicious programs that masquerade as helpful applications. Once installed, they collect and transmit information about you. Hackers and identity thieves use Trojans to steal login names, passwords, and credit card information. A popular method of transmitting Trojans is to disguise them as a "music file" on an Internet site, waiting for someone to download and activate it. They are also frequently disguised as an update to Windows, or even as an update to anti-virus software. Many defense measures, such as anti-virus programs and firewalls, do not detect Trojans. (Webroot, 10/1/03)

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across

networks and bypassing security systems (Webopedia. "Virus" 10/1/03)

Worm

"A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively" (Cole, Fossen, Northcutt, Pomeranz, p. A-148)

Zombie

Computers that contain software that allows an outsider to take over the machine for illicit activities. For example, in a Denial of Service attack, the zombie machines are called by their master to do their masters' (hackers) bidding. (Cole, Fossen, Northcutt, Pomeranz 634). The bidding can be set in the agent/program or be done through a broadcast on the internet. The owners of these zombie machines usually are unaware of their computers extracurricular activities.

Work Cited

- "Cookies." <http://www.leave-me-alone.com/cookies.htm>. 10/1/03
- CERT Coordination Center. "Home Network Security". www.cert.org/tech_tips/hom_network.html. 9/17/2003.
- Cole, Eric, Jason Fossen, Stephen Northcutt, and Hal Pomeranz. SANS Security Essentials with CISSP CBK. Vol. 2.1. SANS Press, 2003 (415, 634, 1206, A-135, A-148)
- Leyden, John. "Worms spread faster, blended threats grow". www.theregister.co.uk/content/56/33151/html. 10/1/2003.
- Microsoft. "Checklist: Install a Firewall". www.microsoft.com/security/articles/firewall.asp. 9/30/2003
- Microsoft. "Frequently Asked Questions About Internet Firewalls". www.microsoft.com/security/protect/firewall.asp. 9/30/03.
- Microsoft. "Internet Connection Firewall Overview". Help Files located locally on Windows XP Professional. 9/17/03
- Microsoft. "Protect Your PC: Print All Three Steps" www.microsoft.com/security/protect/windowsxp/print.asp. 9/30/2003.
- Osterman, Michael. "More problems from infected e-mail". www.nwfusion.com/newsletters/gwm/2003/0811msg1.html. 10/2/2003.
- Rogers, Lawrence. "Use Care When Reading Email With Attachments" http://interactive.sei.cmu.edu/news@sei/columns/security_matters/security-matters.pdf. 10/21/2003.
- SANS. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus". <http://www.sans.org/top20/>. Version 4. 10/14/2003.
- SANS. "What are Worms and Viruses and How Do They Work". www.sans.org/resources/managers/viruses.php. 9/15/2003.
- Sturgeon, Will. "Firms still leave security to chance". silcon.com/news/500013-500001/1/6105.html?rolling=1. 9/22/2003.
- Symantec Security Response. "How to Disable or Remove the Window Scripting Host". <http://www.symantec.com/avcenter/venc/data/pf/win.script.hosting.html>. 10/15/2003.
- The SANS Institute. "SANS NewsBites Vol. 5 Num. 38." E-mail to the author. 24 September 2003.
- Webopedia. "Patch". <http://www.webopedia.com/TERM/p/patch.html>. 10/10/2003.
- Webopedia. "Script Kiddie". www.webopedia.com/term/s/script_kiddie.html. 10/10/2003.
- Webopedia. "Spam". www.webopedia.com/term/s/spam.html. 10/10/2003.

Defense for the Home User: The Why & How

Webopedia. "Virus". www.webopedia.com/term/v/virus.html. 10/1/03
Webroot. Readme.txt .SpySweeper program. 10/1/2003.
Webroot. "Updated News". Posted within the SpySweeper program. 10/1/03
Zone Labs. "How to Stop Spyware".
[//download.zonelabs.com/bin/media/pdf/stopspyware.pdf](http://download.zonelabs.com/bin/media/pdf/stopspyware.pdf). 9/25/2003.

© SANS Institute 2003, Author retains full rights.