Introduction to Computer Security

Table of Contents

Introduction

Hello, and welcome to the CaTS' Intro to Computer Security workshop. Today we will be going over the various threats to your home and office computer and ways to prevent those threats. We will be covering viruses, spyware/adware, and proper use of software and hardware firewalls. By the end of the workshop, you should have a good knowledge of the various computer security issues and how to protect yourself.

- In Part 1, we will cover the various types of viruses, how you can get infected, and how to protect your computer from infection.
- In Part 2, we will cover spyware/adware and how to remove it from your computer.
- In Part 3, we will go over the various firewall programs that are available and how they can help you protect your computer.
- In Part 4, we'll talk about some references you can use for computer security.

1 - Viruses

Viruses have been around for almost as long as personal computers. By definition, a computer virus is “a self-replicating program that spreads by inserting copies of itself into other executable code or documents.” Very much like a real virus, a computer virus alters the code of an existing program to “infect” it and begins to replicate itself. Often viruses have a separate function, such as to delete certain files or cause various effects on a computer. There are actually many different types of viruses. These types include:

- **Macro Viruses**: Macro Viruses use commands (macros) embedded in other software to infect and spread to other files viewed by that software. E.g. Word and Excel have macros, and macro viruses can spread by exploiting these commands.
- **Worms**: Worms duplicate themselves and use communications such as e-mail to spread. They can look at your e-mail address book and send themselves to users in your address book.
- **File Viruses**: File viruses attach themselves to other software. When the software is run, the virus loads itself into memory so that it can further infect other files or begin damaging the computer.
- **Trojan Horses**: Trojan Horses are programs that claim to perform a particular function but in fact do something different. E.g. they could infect your computer with a virus or erase your files.
- **Backdoor Trojans**: Backdoor Trojans are programs that allow other computer users to remotely control your computer via a local area network or the Internet.
- **Boot Sector Viruses**: Boot Sector Viruses are an older type of virus and not so common. They are used to infect a computer's startup program so that the virus would become active as soon as the computer started up.

The most common type of virus today is the Worm. Well known viruses such as the "I Love You" virus and "Bagle" are worms. They spread themselves via e-mail attachments. When the user opens the attachment, it infects the computer. It then sends an e-mail with itself as an attachment to everyone in that computer’s e-mail address book. Worms are also often designed to use up resources on that computer, such as memory and processing power. Once infected, a computer will run considerably slower and often strange errors will appear. If infection is allowed to go on long enough, a computer can become unusable.

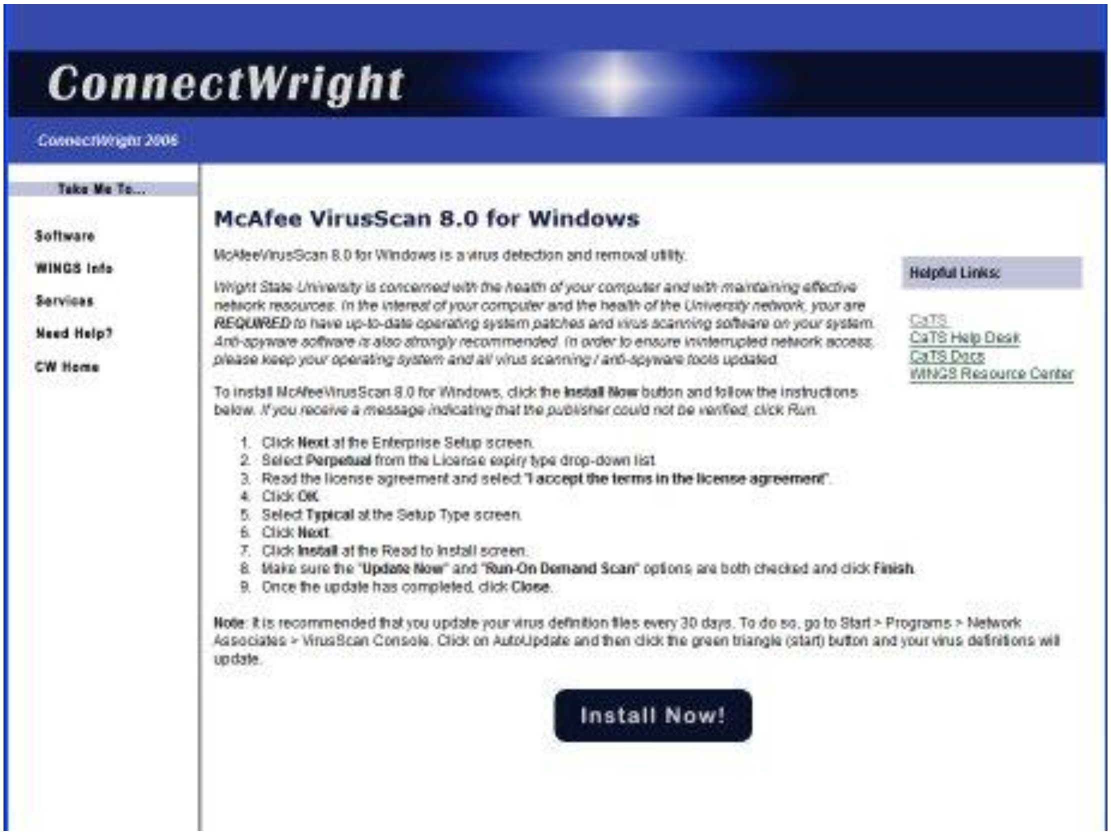
Another very popular type of virus is the Backdoor Trojan. This is a virus, often disguised as another useful program, that gives remote access to your computer to a malicious user. The malicious user can then load programs on that computer, such as a keystroke logger, to obtain passwords and credit card numbers. Obviously this is a very bad thing and why it is very important to use an Anti Virus program on your computer.

Virus Scanners

There are many antivirus programs currently available. The two most popular AV (antivirus) programs, McAfee VirusScan and Norton AntiVirus, often come pre-installed on new computers. At Wright State University, we use McAfee

Enterprise version 8. Other popular, though less well known, antivirus programs include AVAST and NOD32. Because we use McAfee on campus, and because we offer it for free on our ConnectWright website, I will be covering how to update and run McAfee. Other antivirus programs tend to be very similar, so if you use something else, this should help you as well.

To install the McAfee VirusScan from our ConnectWright website, go to the following website address: **https://www.wright.edu/cats/cw/.** Log in using your CAMPUS username and password. Click on the Software link on the left, scroll down and click on VirusScan 8, and then click on Install Now. You should see the screen shown in Figure 1.



McAfee VirusScan 8.0 for Windows

McAfeeVirusScan 8.0 for Windows is a virus detection and removal utility.

Wright State University is concerned with the health of your computer and with maintaining effective network resources. In the interest of your computer and the health of the University network, your are ***REQUIRED*** *to have up-to-date operating system patches and virus scanning software on your system. Anti-spyware software is also strongly recommended. In order to ensure uninterrupted network access, please keep your operating system and all virus scanning / anti-spyware tools updated.*

To install McAfeeVirusScan 8.0 for Windows, click the **Install Now** button and follow the instructions below. *If you receive a message indicating that the publisher could not be verified, click Run.*

1. Click **Next** at the Enterprise Setup screen.
2. Select **Perpetual** from the License expiry type drop-down list.
3. Read the license agreement and select "**I accept the terms in the license agreement**".
4. Click **OK**.
5. Select **Typical** at the Setup Type screen.
6. Click **Next**.
7. Click **Install** at the Read to Install screen.
8. Make sure the "**Update Now**" and "**Run-On Demand Scan**" options are both checked and click **Finish**.
9. Once the update has completed, click **Close**.

Note: It is recommended that you update your virus definition files every 30 days. To do so, go to Start > Programs > Network Associates > VirusScan Console. Click on AutoUpdate and then click the green triangle (start) button and your virus definitions will update.

Figure 1

To install McAfee, just click the button labeled VirusScan 8.

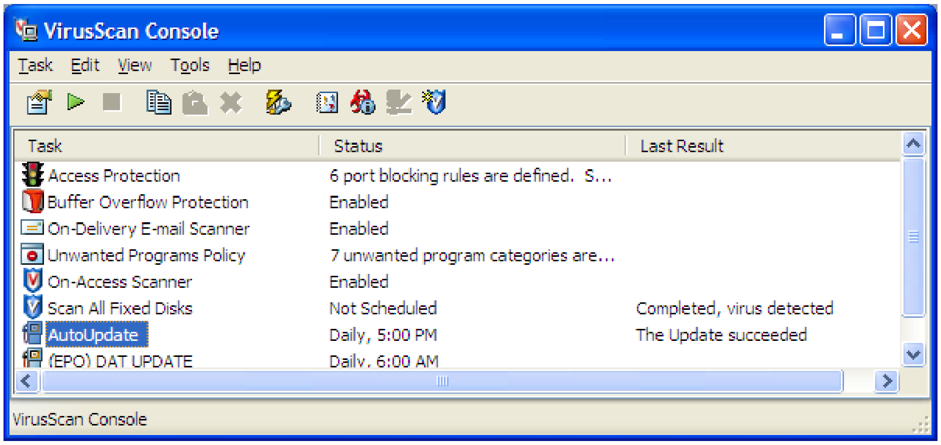
Simply follow the prompts. It should ask you to choose either a Typical Installation or a Custom Installation. Choose Typical, and it should be installed automatically. If you are a more advanced user and want more control over the installation process, choose Custom Install.

Once the install is done, it will ask you if you want to "Run a Full Scan," "Update Definitions," and "Read the Readme File". Uncheck the Readme option, but leave the other two options checked. This will force the program to update itself (this is very important!) and run a full scan of your hard drive(s).

In order to run a Virus Scan on a specific drive or file, all you need to do is right click on that file or drive and click Scan for Viruses. This will start the scan. If you wanted to scan your C: drive, just go into My Computer, right click on the C: drive, and click Scan for Viruses.

There are two more important things to discuss about virus scanning: updating the virus scanner and scheduling it to run automatically.

Updating McAfee is very simple. First, click the Start button to open the Start menu. Go to Programs/All Programs, and find the folder called Network Associates. You will have three options: VirusScan Console, VirusScan On-Access Scan, and VirusScan On-Demand Scan. We want the VirusScan Console. The window will look like Figure 2.



Task	Status	Last Result
Access Protection	6 port blocking rules are defined. S...	
Buffer Overflow Protection	Enabled	
On-Delivery E-mail Scanner	Enabled	
Unwanted Programs Policy	7 unwanted program categories are...	
On-Access Scanner	Enabled	
Scan All Fixed Disks	Not Scheduled	Completed, virus detected
AutoUpdate	Daily, 5:00 PM	The Update succeeded
(EPO) DAT UPDATE	Daily, 6:00 AM	

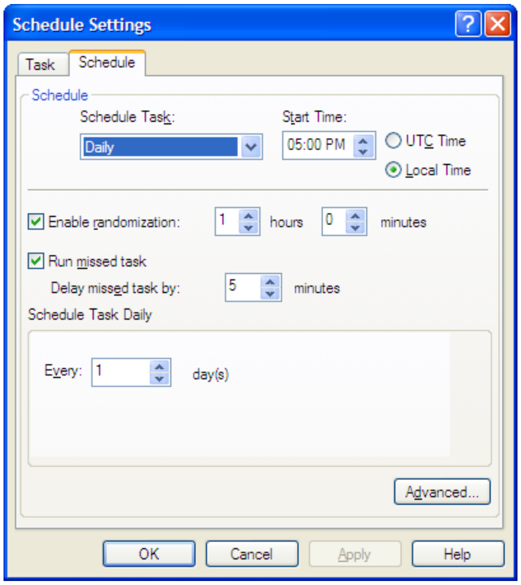
Figure 2

What we want to do is run AutoUpdate. Simply click on AutoUpdate to highlight it, and click on the green triangle button on the toolbar. This will start the AutoUpdate. Make sure you are connected to the Internet when doing this.

To actually run the VirusScan, do the same thing with the Scan All Fixed Disks option. Click on it to highlight it, and click the green triangle button to start it.

This is all well and good, but we don't want to have to remember to do this every day or even every week. This brings us to Scheduling. You can schedule any task that is in the VirusScan console, so we're going to want to do this with the Scan All Fixed Disks option too.

To schedule a task, right-click on the task you want to schedule and click on Properties. It will open the Properties window for that item. You should see a button called Schedule on the right side. Click that, and then click the Schedule tab at the top, and you'll see a screen like Figure 3.



Schedule

Schedule Task: Daily

Start Time: 05:00 PM

○ UTC Time

● Local Time

☑ Enable randomization: 1 hours 0 minutes

☑ Run missed task

Delay missed task by: 5 minutes

Schedule Task Daily

Every: 1 day(s)

Figure 3

When it comes to updating our virus definitions, we want the latest and greatest. If you don't have the most recent definitions, your virus scanner won't be able to catch the newest viruses. In other words, if your definitions aren't up to date, you may as well not have virus protection. So in this case, we want to schedule the update to run every day. You can choose any time you want the update to run, but make sure your computer will be on during that time. You can set it to run a missed task again, but you can only delay it by 30 minutes. If you have the update set to run at 3 am, and you never leave your computer on at night, the AutoUpdate will never run.

You'll want to repeat the scheduling for the task called Scan All Fixed Disks as well. This is the task that scans all of your hard drives for viruses. It is generally safe to set this to run once every week. VirusScan is always working and will generally catch viruses as soon as they appear on your computer. However some do slip through the cracks, and Scan All Fixed Disks is much more thorough than the always-on scanner.

2 - Spyware

Spyware is a bit of a catch-all term for software that is installed on your computer without your knowledge and, often, consent to perform various tasks. Three of the major types of spyware are listed here:

Adware

Adware is to internet browsing as spam is to e-mail. Adware can profile your online surfing and online shopping habits, place annoying pop-up adverts, or install additional IE menu helper bars. Often, adware revolves around targeted advertising based upon the web sites you frequent, and you may not even be aware that the pop-ups are not coming from the actual web site visited itself but from the adware software running locally on your machine. Quite often, these applications are installed by stealth or by deliberately misleading users to install software that is not required.

Spyware

Spyware is potentially a higher threat than adware as it often collects user details, such as software installed, sensitive information such as passwords, and even credit card details, which are then sent to a central collection point via the internet. Spyware is often installed covertly or by accident from pop-up windows with ActiveX controls that report that they are doing something benign whilst secretly installing this malicious software.

Page Hijackers

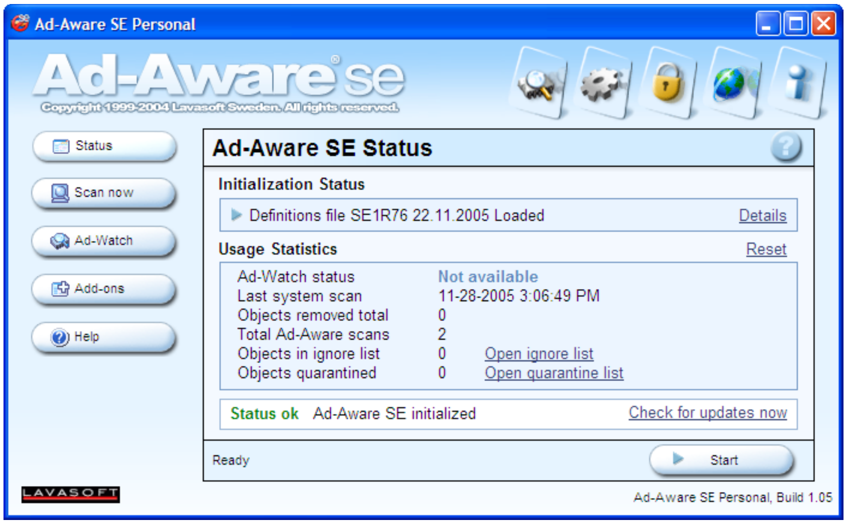
Are applications that redirect links to specific web pages, such as a request to go to a search engine for example, and instead redirect the web browser to a designated address related to the initial link but often containing advertising or adware. While not as high a threat as spyware, it is often a sign that your computer has some spyware or adware components installed on it, which will undermine its operation.

Spyware can be installed on your computer in many different ways. Oftentimes you may be browsing the web when a popup window that looks convincingly like a Windows system message says that your computer is unprotected and to click here to protect it. This is a popup ad to install software that you most assuredly don’t want. Spyware can also be installed along with other programs that are downloaded. Big culprits include WeatherBug and the toolbars that are created for Internet Explorer. WeatherBug is a definite no-no. It may seem very handy, and it is, but it installs all kinds of problematic software along with itself. Other examples include the MSN Search toolbar or a lot of the popular peer-to-peer programs such as Kazaa and Limewire.

All kinds of spyware are annoying, as well as potentially dangerous. Identity theft is becoming more and more common lately, and we definitely need to protect ourselves. It is also very important to take care of spyware sooner rather than later. When you start noticing the symptoms of spyware, don’t think that you can take care of it later. Oftentimes spyware will regenerate and duplicate itself, gradually becoming harder and harder to remove. The sooner you act, the easier it is to take care of. Thankfully, there are many spyware scanners on the market today, and a good number of them are free. I will be discussing how to install and use two of the free products, Ad Aware SE Personal, and Microsoft AntiSpyware.

Spyware Scanners

Two of the most popular spyware scanners available, and the two we use most often on campus, are Ad Aware SE Personal and Spybot Search & Destroy. Both can be downloaded for free from the Internet. Either search for them on Google, or go to http://www.download.com and search for them there. Both can be downloaded from that site. The easiest way to obtain them, however, is to install them from the ConnectWright website (https://www.wright.edu/cats/cw/). They are both listed on the same screen where we found McAfee VirusScan. Instead of Spybot, however, I'm going to cover a new antispyware program that is available from Microsoft, Microsoft Antispyware.



Ad-Aware SE Status

Initialization Status

Definitions file SE1R76 22.11.2005 Loaded Details

Usage Statistics Reset

Ad-Watch status	Not available	
Last system scan	11-28-2005 3:06:49 PM	
Objects removed total	0	
Total Ad-Aware scans	2	
Objects in ignore list	0	Open ignore list
Objects quarantined	0	Open quarantine list

Status ok Ad-Aware SE initialized Check for updates now

Ready

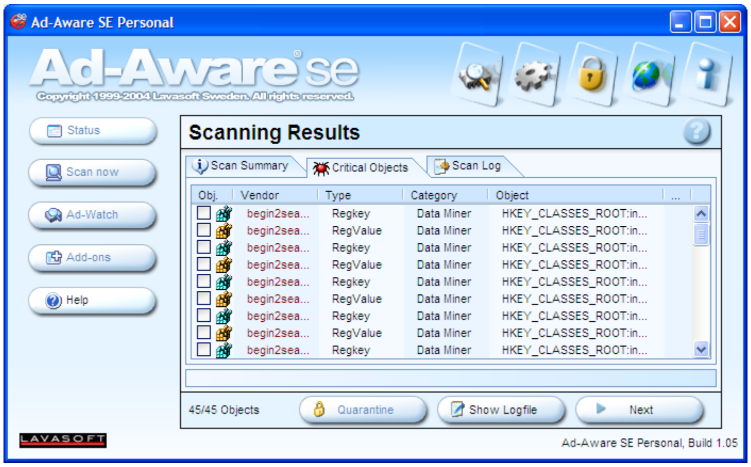
Ad-Aware SE Personal, Build 1.05

Figure 4

We'll start with installing Ad Aware (Figure 4). To start the process, click on the Install Ad-Aware button on the ConnectWright website. When the installer prompt comes up, click Next. On the next screen, check the box next to I Accept, click Next, and then choose Next on the succeeding screen. If given the option to install only for yourself or anyone who uses the computer, choose anyone, click Next and then Next again. The installation will start. Once it is finished, you'll be presented with the final screen.

Uncheck the box next to "Open the help file now," and click Finish. Ad Aware will automatically update itself with the newest definition files, and then start a full system scan. Allow the scan to complete. This may take several minutes.

Once the scan finishes you will be presented with the following screen (Figure 5):



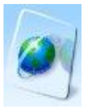
Obj.	Vendor	Type	Category	Object	...
□	begin2sea...	Regkey	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	RegValue	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	Regkey	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	RegValue	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	Regkey	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	RegValue	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	Regkey	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	RegValue	Data Miner	HKEY_CLASSES_ROOT:in...	
□	begin2sea...	Regkey	Data Miner	HKEY_CLASSES_ROOT:in...	

45/45 Objects

Figure 5

Figure 5 displays the items found from the scan. To remove them, simply right click in one of the check boxes next to any item and choose Select All Objects. Then click the Next button. It will then quarantine and delete the items selected.

In the future, if you want to update Ad Aware, and you will need to do this whenever you scan with it, simply open the program, and click on this icon:



Then, click on the Continue button and Ad Aware will check for new updates, download them, and install them automatically.

To run a full scan, open the program and click the Start button. Choose Full System Scan and click Next.

Generally it isn’t as important to run spyware scans as often as virus scans, but it is still something you want to do every so often. I suggest at least once every month; more if you start having noticeable problems, such as popups or browser highjacks.

3 - Firewalls

From Webopedia.com, a firewall is defined as "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria."

Firewalls are vitally important to network and Internet security. There is a lot of malicious network traffic going around, from viruses attempting to find vulnerable computers to infect, to malicious users trying to worm their way into a network. A firewall, either software or hardware, can be an invaluable tool to prevent those unwanted intrusions.

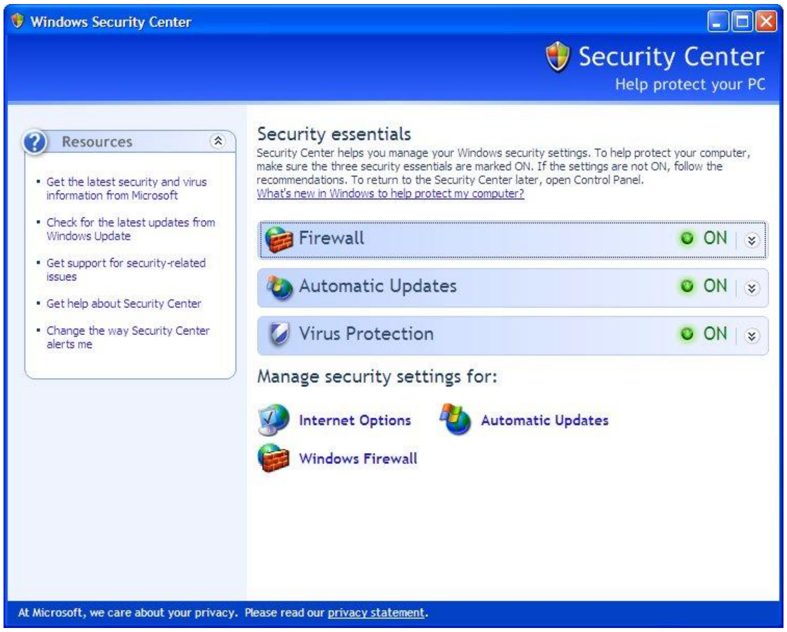
Hardware firewalls come in many forms. Firewalls for large networks are generally servers dedicated to the task of filtering network traffic, and they are generally one of the first computers that a data line will be hooked to in a network. For home networks, routers are often firewalls as well. As broadband Internet is becoming more popular, and more and more homes have multiple computers, cable and DSL routers are becoming quite common. Popular brands include D-Link, Netgear, and Linksys.

These firewalls often work by simply blocking incoming traffic through certain "ports." A port number indicates the type of traffic that is passed through a network. For example, port 80 is often associated with HTTP traffic, or World Wide Web traffic. When you download a web page, it is usually downloaded through port 80. However, hackers will search for open ports to upload malicious code to a computer. A router firewall prevents this by blocking off all but the most common ports. It's like locking your doors and windows before going to bed at night. If they're left unlocked, it's easy for an intruder to get in your house. The same goes for your computer. The administrator of the firewall can always open any ports that are necessary.

Software firewalls are programs that run on an individual computer that blocks access to that specific computer. Examples of software firewall packages include Microsoft Windows Firewall, McAfee Desktop Firewall, Norton Internet Security, BlackICE, and ZoneAlarm. These programs work similarly to hardware firewalls, in that they block access through specific ports, but they also block individual programs from accessing the Internet. After installing a software firewall, when you run a program that requires access to the Internet, the firewall program will prompt you asking if you want to allow that program to have access. You can usually say "Yes, this time," "Yes, every time," "No, this time," or "No, every time." This allows you to control which programs have access and which do not. This is very useful, because if a virus infects your computer, a firewall can help to prevent it from spreading to other computers on your network.

Windows Firewall

The Microsoft Windows Firewall is a feature included with Windows XP Service Pack 2. It is generally a very unobtrusive firewall that stays in the background most of the time. You can access the Windows Firewall by opening the new Security Center control panel. Just go to the Start Menu and go to the Control Panel. You should see an icon labeled Security Center. Open it and you will see the screen displayed in Figure 6.



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

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

Firewall ● ON

Automatic Updates ● ON

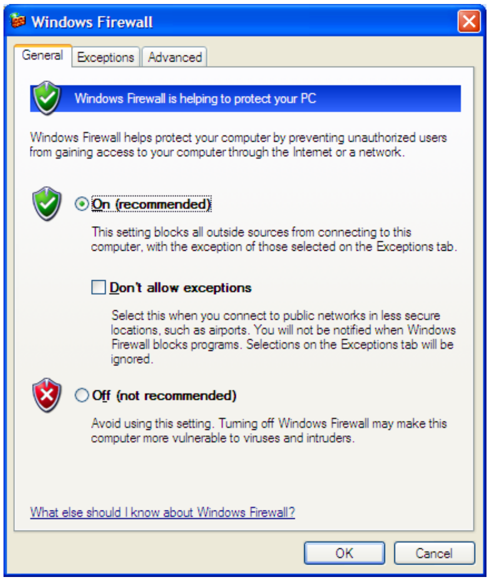
Virus Protection ● ON

Manage security settings for:

At Microsoft, we care about your privacy. Please read our privacy statement.

Figure 6

You'll see that the Firewall is listed as ON. This is the way we want it to be. If it is OFF, simply click on the Windows Firewall icon at the bottom of the window. The screen shown in Figure 7 will display.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

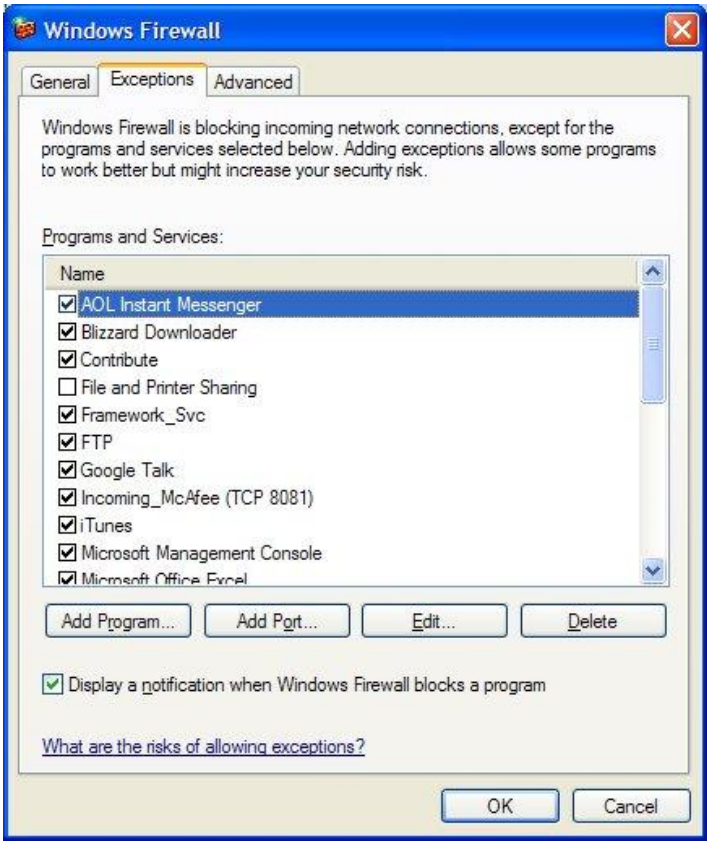
○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Figure 7

If the firewall is set to Off, simply click On and hit OK. To turn the firewall off, simply do the opposite. To alter the programs that have access to go through the firewall, click on the Exceptions tab (Figure 8).



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name

- ☑ AOL Instant Messenger
- ☑ Blizzard Downloader
- ☑ Contribute
- □ File and Printer Sharing
- ☑ Framework_Svc
- ☑ FTP
- ☑ Google Talk
- ☑ Incoming_McAfee (TCP 8081)
- ☑ iTunes
- ☑ Microsoft Management Console
- ☑ Microsoft Office Excel

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Figure 8

This screen allows you to check or uncheck any program you want to allow or disallow access to the network. You can also manually add a program using the Add Program button, or add a port number with the Add Port button. So if you know a specific port number that needs to get through, you can add that number to the list. Once all necessary changes have been made, just hit OK. You should now have a good grasp on how to use the Windows Firewall.

4 - References

Helpful Links

ConnectWright Website (Software Downloads)
https://www.wright.edu/cats/cw/

Information Technology (IT) Security Website
http://www.wright.edu/security