Protecting Your Computer

A Basic Home Security Guide

COPYRIGHT

TERMS OF USE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document was created with the intention of helping users identify and understand some of the basic threats that come with owning a computer; specifically viruses, spyware, and intrusions from third parties. Our audience is the average home user whose goal is to secure their home network, but does not necessarily need to or want to know the intensive details and definitions of such technical topics (e.g. how Firewalls technically work).We provide users with a list of possible solutions to help secure their computer and network from these threats, and draw their attention to some specific areas which are commonly overlooked in the process.

This document is not intended for technicians, businesses, or educational institutions. For those users who already have a basic understanding of these threats and solutions, or those individuals who are searching for more in-depth information behind these topics, there are many resources on the internet that will provide you with this type information. For the most part, you will not find that information here, as that is not what our intended audience is in search for. We apologize if we disappointed anyone.

LAYERS OF SECURITY

Protecting yourself on the internet is no longer a corporate issue. It has become a billion dollar industry for hackers and other cybercriminals to infect your home computer, steal your personal information, and use your computer to be part of a robot army to steal even more. Today's home network needs more than just a software firewall and antivirus. By layering your security, you make it harder for those bad guys to get in.

Recommended Layers of Security

- Hardware Firewall/Router
- Software Firewall
- Resident Antivirus
- Resident Antispyware
- Limited User Account
- Content Filtering

VIRUSES

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with the computer's operation. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, steal your personal information, look for other computers on your network to infect, or even erase everything on your hard disk. It has become increasing common for illegally traded software to contain such viruses, so you should avoid partaking in such actions for your own safety. Viruses are most easily spread by attachments in e-mail messages or instant messaging messages and dubious websites. This is why it is essential that you never open e-mail attachments unless you know who it is from, and you are expecting it. Viruses can be disguised as attachments of funny images, online games, greeting cards, or audio and video files. A virus also spreads through downloads on the Internet. Any webpage or downloadable file on the internet could be laced with a virus without your knowledge. (Microsoft)

Every computer should have an up-to-date antivirus client installed and running resident, or in other words running in the background. PLEASE NOTE: You should only have **one** antivirus client running resident at any given time. Do **NOT** run more than one as it will negate the protection both provide! Most of the time you will never notice this software is running. Depending on this software's settings, you will only be notified in certain situations. These circumstances are most commonly when:

1. **The virus definition or the program itself has been updated (or needs to be updated)**. Generally, most antivirus software check for updates at least once every 24 hrs, every 30 minutes is much better. Sometimes the vendor includes a setting allowing you to change how frequently the software checks for updates. You should **NOT** change this setting to be any higher than every 24 hrs. If you do not have the option to control this, you should force updates to your software a few times a day. For example:

    - **When you start your computer**. Usually the software will update itself when the computer first boots up. If not, this would be the best time of day to update, before you start browsing the internet or opening e-mail.
    - **When you go to lunch.** Get ready for the second half of the day by forcing another update. You do not even have to stick around to watch.
    - **Anytime you take a break.** If you walk away for a while and leave your computer on, force an update if you remember.
    - **If you have been on the computer all day**. If you have been on it all day, force an update before you shut down for the night.
    - **If you forget to force an update**, you should update the software and maybe run a quick scan to make sure you did not run across any new viruses.
    - **Make sure your update is complete!** For example Norton will update, but is not complete until it says your software is up to date (this can require several reboots and/or running the update again).

2. **The program scans for viruses.** It is suggested that you scan for viruses at the very least once a week. It is recommended to scan three or four times a week, if not every night. You can set the program to scan overnight so it does not interrupt you. If you have a good antivirus, it should stop the virus before it gets onto your computer, as long as you keep the software update to date. If you suspect your computer has a virus, make sure your software does a **Full Scan** and not a Quick Scan.

3. **A virus is found on your computer.** If a virus is found the software will notify you of the file name, the virus name, and what actions it took to get rid of the virus (if any). These actions usually include placing the file in a secure location so it does not spread (quarantine), removed the infected parts of the file (cleaned the file), or the software removed the infected files all together (deleted the virus). If the software is unable to remove the file, write down its location so you are able to remove it yourself. If it asks you what actions to take, quarantining the virus is usually your best bet. Sometimes poorly designed antivirus clients mistake virus-free programs as viruses. Once the vendor is notified of their mistake, they usually issue an update to correct it (eventually). You can rescan quarantined files and restore safe files in the case of a "false positive" made by your antivirus client.

Some Signs You May Be Infected

This is a list of symptoms collected from Microsoft, ciocentral.org, lockdowncorp.com, in combination with our own personal experiences.

1. Your CD/DVD/Blu-Ray player's drawer opens and closes by itself.
2. Your computer screen flips upside down.
3. Your wallpaper or background settings change by themselves.
4. Documents or messages print on your printer by themselves.
5. Your computer browser goes to a strange or unknown web page by itself.
6. Your windows color settings change by themselves.
7. Your screen saver settings change by themselves.
8. Your right and left mouse buttons reverse their functions.
9. Your mouse pointer disappears.
10. Your mouse moves by itself.
11. Your Windows Start button disappears.
12. Programs load or unload by themselves.
13. Strange Windows Warning, Info, error, or question boxes constantly appear on your computer.
14. Your time and date change on your computer by itself.
15. Your computer shuts down and powers off or reboots by itself.
16. Your Task bar disappears
17. Your account passwords are changed or others can access your accounts.
18. Your security software is shutdown and will not start properly.
19. Your computer monitor turns itself off and on.

20. Your modem dials and connects to the Internet by itself.
21. Your files are in use when you are not accessing them.
22. Your keyboard or mouse freezes
23. Ctrl + Alt + Del no longer works.
24. When you reboot your computer you get a message telling you that there are other users still connected.
25. Your computer slows to a crawl.
26. The computer stops responding, or it locks up frequently.
27. The computer crashes, and then it restarts every few minutes.
28. An antivirus program cannot be installed on the computer.
29. New icons appear on the desktop that you did not put there, or the icons are not associated with any recently installed programs.
30. Websites are unexpectedly added to your Favorites folder.
31. 'Memory low' error messages appear.
32. The Windows Task Manager or MSCONFIG will not open or disappears.
33. The computer takes longer than normal to start up.
34. Documents, programs and other data may mysteriously disappear from the computer.
35. There is a double extension on an attachment that you recently opened (e.g. birthdayparty001.jpg.exe).
36. You get pop-ups telling you that you have been infected and to click on a link to install or buy a removal program.
37. You get the deadly BSOD (blue screen of death). The blue error screen with white text commonly shown for critical Windows errors.

Antivirus Software

Free

If you are unable or would prefer not to pay for antivirus software, there are some free solutions to choose from. This software is free for personal use. Free software is not necessarily the best solution, you get what you pay for, but they do a decent job at protecting your computer. We have to warn you that most free security products have some important features removed. Here is a list of free antivirus software:

- Alwil AVAST
- Avira AntiVir
- Grisoft AVG

Pay

If you are able, it is highly suggested that you go with one of the vendors which offer paid software. They generally range in price from $30 to $60 annually. Some of the most popular vendors are:

- Sophos (5 or more users)

- ESET NOD32
- Kaspersky
- BitDefender
- Malwarebytes Anti-Malware
- McAfee

There are others out there, but these are the most popular, effective solutions you will find. Whether you choose free or pay software, it's always good to back it up with a separate antivirus. If you would like to backup your antivirus software with something, you have three options:

One-Time-Scanners

Download, install, update, and run. This software does **NOT** run resident. It will only scan your computer for viruses when you tell it to, and you may have to update it manually. It is good to use as a backup scanner if you would like to run a backup scan, but do not have an Internet connection available.

- BitDefender
- McAfee
- Microsoft Malicious Software Removal Tool*
- Malwarebytes Anti-Malware (Free)
- RogueRemover (Free)

* Install, and then run by clicking on Start, then Run, and typing "MRT" (without quotes). Software is updated monthly though Windows Update.

Online Scanners

Generally, online scans are better than the "One-Time-Scanners" because you do not need to remember to update the software. The software updates itself so you only need to scan your computer directly through your web browser. It complements the scanners you have installed on your PC and should be used in conjunction with them, especially if one of your scanners finds some form of malware.

- Trend Micro House Call
- BitDefender
- McAfee
- NOD32
- Norton
- Kaspersky Labs

File Scanners

Antivirus software is not perfect, and sometimes files are misdiagnosed as either infected or clean. If you are unsure whether a specific file is clean or not, here are some websites that will scan a single file for you. The first three websites will scan the file with multiple antivirus

programs and show you what was detected (or not). Caution, these sites place a limit of the size of the files you can upload.

- Virus Total
- Jotti
- VirSCAN
- Alwill AVAST!
- Kaspersky

SPYWARE

Spyware is a general term used to describe software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent first. (Microsoft) Spyware is not a virus; therefore antivirus software will not prevent spyware from being installed on your computer. It has become very common for antivirus vendors to include antispyware protection with their programs, so be sure you check your antivirus client to see if it includes this protection.

Once again, every computer should have up to date antispyware software installed and running resident, or in other words running in the background. PLEASE NOTE: You should only have **one** antispyware running resident. Do **NOT** run more than one as it will negate the protection both provide! Most of the time you will never notice this software is running. Depending on this software's settings, you will only be notified in certain situations. These circumstances are most commonly when:

1. **The spyware definition or the program itself has been updated (or needs to be updated).** Generally, most antispyware software checks for updates every 24 hrs. Sometimes vendors include a setting allowing you to change how frequently the software checks for updates. You should **NOT** change this setting to be any higher than 24 hrs.

    - **Make sure your update is complete!** Some software will update, but may require the computer to be restarted before the update is complete.

2. **The program scans for spyware**. It is suggested that you scan for spyware at the very least, once a week. It is recommended to scan three or four times a week, if not every night. You can set the program to scan overnight so it does not interrupt you. If you have a good antispyware program, it should stop any spyware before it gets onto your computer, as long as you keep the software update to date.

3. **Spyware is found on your computer**. If spyware is found the software will notify you of the file name, the spyware name, and what actions it took to get rid of the virus (if any). These actions usually include placing the file in a secure location (quarantine) so it does not affect your computer or removed the infected files (deleted the spyware). If the software is unable to

remove the file, write down its location so you are able to remove it yourself. If it asks you what actions to take, quarantining the spyware is usually your best bet.

PLEASE NOTE: Cookies are commonly marked as spyware. Cookies are used by websites to store information about your browsing habits on their website. This could be anything from saving shopping cart information (if you are buying items online), your log in information (if you selected to stay logged in), or other information along those lines. Some cookies may contain sensitive or personal information (such as passwords, banking information, credit card information, etc.) although most websites have moved away from storing this type of information in cookies. Cookies are only a minor concern, and you can take steps to preventing them completely (although it will affect your ability to access most websites). You can set your browser to prompt for cookies so you will only get the ones you really need or want. Refer to your browsers help section to find out how to do this.

Some Signs You Have Spyware

This is a list of symptoms collected from Microsoft, ciocentral.org, lockdowncorp.com, in combination with our own personal experiences.

1. You see pop-up advertisements all the time.
2. Some settings have changed and you can't change them back.
3. Web browser contains additional components (commonly toolbars) that you did not install.
4. Computer is running slow.
5. The homepage of your browser is changed.
6. Your firewall alerts you to an unknown program trying to access the Internet.
7. Your security software is shutdown and will not start properly.
8. Every time you do a search, you wind up at the same unusual and unknown web site search engine.
9. There is a new program or multiple programs in the Add/Remove Programs section of your control panel that you did not install.
10. The Windows Task Manager or MSCONFIG will not open or disappears.
11. Your computer browser goes to a strange or unknown web page by itself.
12. Your keyboard or mouse freezes
13. Ctrl + Alt + Del stops working.
14. Your computer slows to a crawl.
15. The computer stops responding, or it locks up frequently.
16. New icons appear on the desktop that you did not put there, or the icons are not associated with any recently installed programs.
17. Web pages are unexpectedly added to your Favorites folder.
18. The computer takes longer than normal to start up.
19. You get a lot of returned emails from people you don't know.

20. There are warnings appearing that your computer is infected with a virus or is insecure. These messages usually include a link to an unknown website telling you to install or purchase their software.

Antispyware Software

Free

If you are unable or would prefer not to pay for antispyware software, there are some free solutions to choose from. This software is free for personal use. Free software is not necessarily the best solution, you get what you pay for, but they do a decent job at protecting your computer. We have to warn you that most free security products have some features removed. Here is a list of free antispyware software:

- Windows Defender (Comes preinstalled on Microsoft Vista)
- Spyware Terminator
- SuperAntispyware
- Spybot Search and Destroy

Pay

If you are able, it is highly suggested that you go with one of the vendors which offer paid software. They generally range in price from $20 to $40 annually. Some of the most popular vendors are:

- Spyware Doctor
- Spy Sweeper
- CA eTrust PestPatrol
- Malwarebytes Anti-Malware
- Adaware (Plus or Pro)

There are others out there, but these are the most popular, effective solutions you will find. Whether you choose free or pay software, it's always good to back it up with separate antispyware scanner. If you would like to backup your antispyware software with something, you have two options:

One-Time-Scanners

Download, install, update, and run. This version of the software does **NOT** run resident. It will only scan your computer for spyware when you tell it to, and you may have to update it manually. It is good to use as a backup scanner if you would like to run a scan, but do not have an Internet connection available.

- Adaware (Free)
- Malwarebytes Anti-Malware (Free)
- Microsoft Malicious Software Removal Tool*

- RogueRemover (Free)

* Install, and then run by clicking on Start, then Run, and typing ”MRT” (without quotes). Software is updated monthly though Windows Update.

Online Scanners

Generally, people tend to stick with the “one-time-scanners” as backup spyware protection. There are some online scans available, and you do not need to remember to update the software while using these. The software updates itself so you only need to scan your computer directly through your web browser. It complements the scanners you have installed on your PC and should be used in conjunction with them, especially if one of your scanners finds some form of malware.

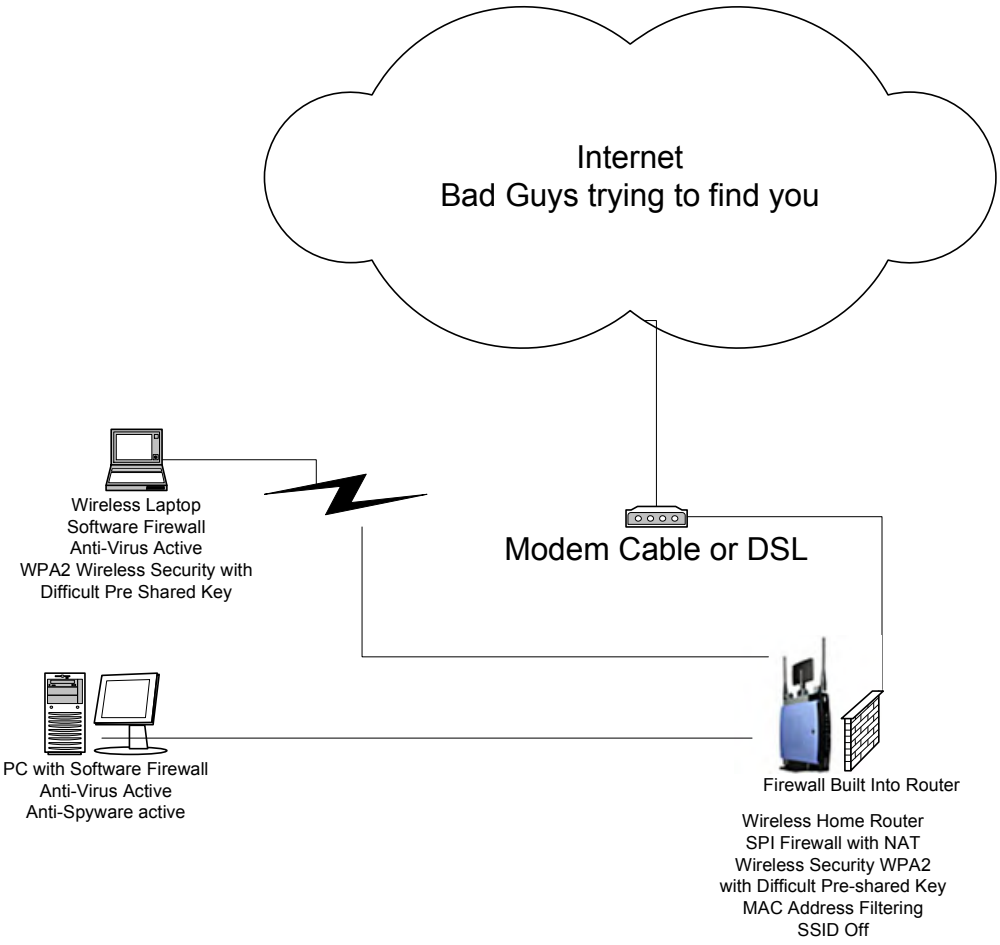
- Trend Micro House Call
- CA Spyware Scanner
- Microsoft Safety Scanner use the safety scan only, choose full service scan. We do not at this time recommend installing OneCare as your primary software protection, but safety scan is another tool in your arsenal.

FIREWALL

You can think of a firewall as a brick wall. You are on one side of the wall, and on the other side is everyone else. Anyone wanting to get to your side of the wall cannot, but you have the ability to place a door anywhere along the wall to let people through. Unfortunately, some computer users never build this wall, or even worse, place doors, windows, and ladders all along the wall without even knowing it.

Every computer needs a minimum of a software firewall, but layering your firewall protection is a better idea. Combining a hardware firewall with a software firewall will make it harder for anyone to get to your computer; you can think of it as adding a second brick wall between you and them. This will also prevent a complete security failure in the event an update to your operating system (Windows) or firewall has a flaw, causing one of the firewalls to stop protecting you.

Firewalls come in many flavors, and for home users they are now included with their broadband routers. Today’s routers should include SPI (Stateful Packet Inspection) not just NAT (Network Address Translation). If you have an older broadband router it may only have NAT, and in this day in age that is not enough! It would be time to upgrade to a newer model. More and more of the routers on the market offer wireless internet access which needs its own security configuration to keep you safe. Check with your manufacturer about any older model you may have, or look up the specifications for your model on their web site.



This is a diagram of a sample home network with layered firewalls. There is one firewall built into the router, and one software firewall installed on each machine. It is **NOT** recommended to connect directly to your Cable or DSL modem.

- Basic Hardware/Software definition

Hardware Firewalls

If you are unsure whether you have a hardware firewall or not, let's keep it simple. If you own a broadband router, you probably have a hardware firewall. For your protection, all newer routers have firewalls built right into them and usually come with software to help you configure it. The security settings available to you depend on the age and brand of router you own. If you own a several year old router, you should consider purchasing a newer one for the enhanced security features.

You should read through all of the documentation provided with your router to become familiar with the security features it offers and any recommendations made by the manufacturer. Out

of the box, routers are usually setup with "factory settings." These are the default settings the manufacturer has found to work, but not necessarily recommended. Usually, these settings need to be changed to better suite your security needs.

Important things to remember:

- No router is up to date out of the box; you need to update the firmware when you get it. This is like getting the latest operating system updates to protect your computer, and you should check for updates on a monthly basis.
- Each router has its own firmware (or patch) depending on the make, model, and version number.
- Security is not simply taking the router out of the box and plugging your modem and computer into it; there are more steps. The most important step you should take is changing the default password for the administrator login to the router before you connect it to the modem. It does not matter whether you have a cable or DSL connection; you need to change the password first. This is especially important if your router has wireless capability. You do not want your neighbor or anyone else taking control of your network.

Tips for a good password

- Make it easy for you to remember, or write it down and put it in a safe with your other valuables. Easy to remember does not mean an easy password that can be guessed or cracked.
- Longer passwords are better, try to keep the password to 8 or more characters long.
- Make it difficult for someone to figure out. Do not use pet or family names, birthdays, or other personal information.
- Use uppercase and lowercase letters combined with numbers and special character such as ~.
- "Password", "Secret", or anything like that, is not a good password.
- Avoid words that are in the dictionary, unless you combine those words in a clever manor that makes a nonsense word. For example Fish@Pie~94Heaving (of course don't use this one it's just an example).

How to Change Routers Settings

There are a couple of ways to access the settings of your router. PLEASE NOTE: You will need the username and password of the router in order to access these settings. To find the default username and password of a router, check the documentation that came with the router or the manufacturer's website. You can also check the list on phenoelit-us.org.

1. **Manufacturers Website.** The manufacturer may have provided you with a web address you could use to access the routers settings. Search through the documentation provided with your router to see if an address is provided for you.

2. **Routers IP Address.** The most common way to access these settings is using the routers IP address. Usually this address is either 192.168.1.1 or 192.168.0.1. To check which one you will need, check your documentation, use the manufacturer's website, or follow these steps:

    - Click on Start, then Run, and type "`cmd`" (without the quotes) and hit OK.
    - In the command prompt, type "`ipconfig`", hit enter, and look for the Default Gateway. That is the IP address of your router.
    - Open Internet Explorer and type in the IP address exactly as it is shown in the command prompt to access the router's settings.

3. **Basic Settings to check.**
    - Update the firmware.
    - Change the default administrator's password.
    - Using a DSL router from some companies, like Verizon, you need to add your login ID and password and change the default IP address of the router. (So if the default is 192.168.1.1 it could be changed 192.168.2.1)
    - Make sure the log is enabled. This will allow you to see who was trying to access your network and where anyone using your network went.
    - Enable MAC address permissions and include the MAC address of each computer accessing the router.
        - How to find the MAC address
    - For wireless routers, enable wireless security (we will discuss this later).
    - Make sure you are set to the correct Time Zone.
    - When finished, backup your settings.

Software Firewalls

Once again we recommend you layer your protection by having one hardware and one software firewall. PLEASE NOTE: If you have Windows XP or Windows Vista, you already have a software firewall included with your operating system (Windows Firewall). **If you are installing a different firewall, make sure Windows Firewall is disabled after the installation is complete. Most good programs will do this for you.**

- How to disable Windows Firewall in XP
- How to disable Windows Firewall in Vista

Free

If you are unable or would prefer not to pay for firewall software, there are some free solutions to choose from. This software is free for personal use. Free software is not necessarily the best solution, you get what you pay for, but they do a good job at protecting your computer. We have to warn you that most free security products have some features removed. Here is a list of free firewall software:

- Comodo
- Online Armor
- Jetico version 1.1
- ZoneAlarm Free Firewall
- Sunbelt Personal Firewall
- Windows Firewall – Built into Windows XP and Vista. The version included with XP only offers inbound protection as opposed to the inbound and outbound protection offered by all other firewall software.

Pay

If you are able, it is highly suggested that you go with one of the vendors which offer paid software. They generally range in price from $10 to $40 annually. Some of the most popular vendors are:

- Online Armor
- ZoneAlarm Pro
- Sunbelt Personal Firewall Full
- Jetico 2.0
- Outpost

Wireless Security

Wireless Standards

The standards that have been approved are A, B, and G. As of this date the Wireless-N standard has yet to be agreed upon, but the throughput is much faster (speeds 270 Mbps compared to the current 54 Mbps). What is important is that you obtain the latest approved standard, unless you like to try new things. You can consider the Wireless-B standard retired, and you should not purchase a Wireless-B only router. What is more important is the encryption capability of your wireless router and the wireless card in your computer.

Types of Wireless Security

Depending on the age of your router and the wireless card you own, different levels of encryption will be available. The settings available to most home users will be WEP, WPA, and WPA2. WPA2 is the strongest of the three, and is recommended over the other two. Older hardware may force you to go with an older, less safe encryption method. You can consider this

a weakness, so it is better to upgrade to newer hardware if possible. Try to avoid WEP if you can because your password can be cracked very easily.

Configure the Wireless Router

Now that you have secured everything you can connect to the router with your laptop and enjoy working anywhere in your home, but if you have not restricted the wireless connection anyone, including your neighbor, can join you without your knowledge. Hopefully by now you have changed the default administrator's password with something complicated; now you need to ensure the only people who have access to your network are approved by you! To do this, you will need to change the settings of your wireless signal by encrypting the signal (WIFI security) and making it harder to find and access your network. You need to log into the router to change your wireless security settings, so have your routers login information nearby. Here is a list of things to check:

- The SSID is the public name given to your network. If you have to broadcast your SSID change it something that makes no sense to anyone but you (by default it will be the brand of your router). If you "broadcast" it, anyone with a wireless card will be able to see that your network is in range, which means encryption needs to be turned on.
- If you have the right wireless card and driver, you can turn the broadcast off, which makes it harder to find your network.
- Wireless Security Encryption needs to be enabled on your router and it should be the highest encryption available for your equipment (again we recommend WPA2 with a long password that has a mixture of special characters, lower case and capital letters, and numbers in it).
- Select the strongest encryption your systems will accept. We recommend **avoiding** WEP since it can be broken into very easily. To emphasize once more, the best bet for the home user is **WPA2** with pre-shared key using a long difficult password.
- Enable MAC address permissions and add the MAC address of each machine allowed on the network.

  How to find the MAC address

Your wireless card can pose an additional risk as well. There are two options you should disable to help further secure your system: Disable the automatic connect feature, and turn off Ad Hoc connections.

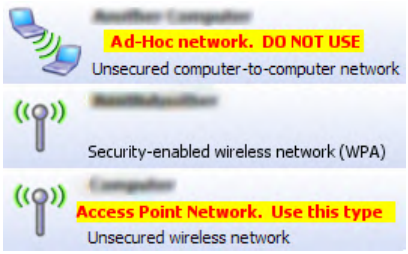
- Windows XP

  In Windows XP. Click on Start, then Run, and then type "`ncpa.cpl`" (without quotes). Once there, right click the wireless network icon and choose Properties. Click the Wireless Networks tab and then the Advanced button near the bottom of section. Under the "Networks to Access" section, select the second option (Access

point networks only). Next, remove the checkmark from the "Automatically connect to non-preferred networks" box and click close, and then OK.

- Windows Vista

  In Windows Vista. You're in luck! Windows Vista will force you to manually connect to networks. It even goes the extra step to tell you the network is an "Ad-Hoc Network" or not.



On a final note, we must remind you to only connect to networks you trust. When you connect to an open network, you are exposing yourself to unknown dangers. Any information you send over that network could be stolen in the process (this includes passwords, banking information, credit cards, and other sensitive information). Be especially careful when deciding to use public computers. There is no telling who has used the computer before you, or who will use it after.

SECURITY SUITE

A security suite is a combination of several security programs, usually consisting of an antivirus, antispyware, antispam, and a firewall, grouped into a single package. They are often cheaper to buy, when compared to purchasing each of the products individually, and have the benefit of only requiring you to check one product for updates instead of three or more.

Security suites should be selected on the basis of the company's reputation with the products in the suite. Some vendors who offer security suites have a lot of experience in one area of protection (e.g. virus protection), and not so much in the other areas. This usually leads to a difficult decision of whether or not to completely rely on a single vendor for your protection. We suggest you go with the vendor(s) that **you** trust; it is your security that is at risk, so do your research before making the decision.

The costs of these products tend to range from $45 to $70 annually.

- Sophos Security Suite (5 or more users)
- ESET Smart Security
- McAfee Internet Security
- Kaspersky Internet Security

- BitDefender Internet Security/Total Security
- ZoneAlarm Internet Suite

If you use a security suite that has a firewall and plan to share local drives or printers, you need to configure the local firewall to recognize the network in your home. Check with the manufacturer for changing that setting.

MISCELLANEOUS SECURITY TOOLS

There are other tools available you could use to increase your computer's security. Without going into every single type of these, we will touch on a few basic ones that we feel computer users should use.

Hosts File

The Hosts file is a file on your computer that contains a local listing of the IP addresses of websites and other networks. If that does not mean much to you, don't worry about it. The only thing you have to remember is that this file can be used to stop your computer from accessing dangerous websites. How? Well, if you were to accidently click on a link which would normally take you to a website known for infecting computers or containing malicious software, you can set your Host file to not load this page. Viruses and spyware can also use this file in exactly the same way, although with harmful goals in mind.

Now it is impossible for me or you to know all the various websites that are harmful, so we rely on professionals. There are a couple programs you can use to update the Host file so it has the latest listing of these known bad websites:

- Hosts File Updater
- HostsMan
- HostsXpert
- ZonedOut

All of these products do generally the same thing, download their Host file and replace yours with theirs. Some offer more features than others, such as sorting and searching, manual editing, and locking the Host file to prevent malware from making changes. We suggest locking the Host file if you are given the option.

The Host file does not need to be updated very often. Checking for an update every week would be more than enough to keep you safe. You should also notice a large decrease in the amount of advertisements you see while surfing the internet as well.

PLEASE NOTE: After updating the Host file you may notice an increase in the number of items on webpage's or complete websites that will not load. You may receive a "Webpage cannot be displayed" error in their place. This is normal, and nothing to be concerned with. This means either the server hosting the website is either not working (try again later), or the site was listed in your Host file and was

blocked for your safety. More often these elements are completely removed from the page (no error will be disabled) and you won't even realize they were there in the first place.

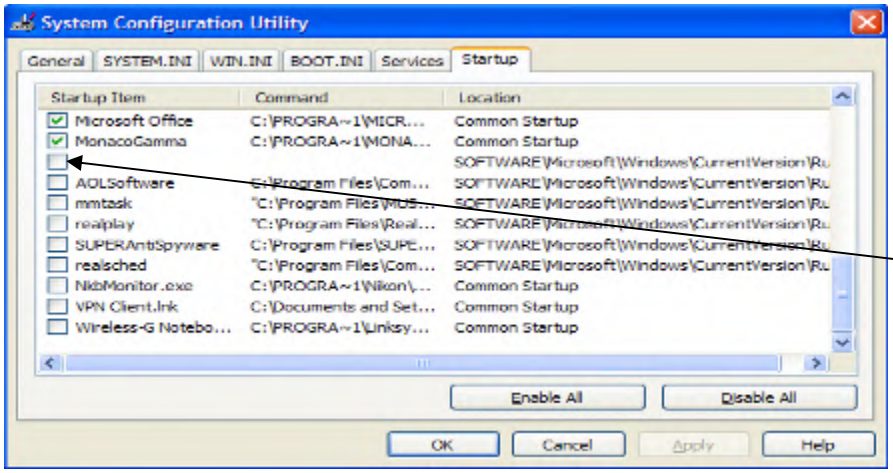
I THINK I'M INFECTED! WHERE DO I START?

Calm down and take a deep breath. The first step is always the most important; realizing you can get a virus. No Operating System (e.g. Windows, Macintosh, Linux, etc.) is safe from these threats, regardless of what you may have heard. Unfortunately Windows is the most targeted Operating System since it is the most widely used, so we will focus our attention there. So, where should you start?

1. Try to update your antivirus and antispyware programs. There are some nasty viruses out there that may prevent this. In those situations, you can skip this step for now and come back to it after you remove that virus.
2. If you are running any version of Windows (e.g. XP, Vista, 7, etc.), turn off your system restore. You do this because your restore points have probably been infected too, and they are of no use to you at this point. Once you have cleaned your computer from all infections, you can start system restore again.

    - How to turn off System Restore (Windows Vista)
    - How to turn off System Restore (Windows XP)
    - How to turn off System Restore (Windows ME)

3. Click on Start, then Run, and type `MSCONFIG` then hit OK. Under the Startup tab, check for programs running with no description. Remove the checkmark next to them so they do not run when your computer starts.



Uncheck blank items

Google the ones you don't know to see if they are OK

If you do not know what some of the programs are, Google them, or try searching a startup database to make sure they are safe. Some startup databases are below:

- Sysinfo.org

- Networktechs.com
- Bleepingcomputer.com
- Windowsstartup.com

4. If you can update all your antivirus and antispyware programs, boot your machine into **Safe Mode** and begin running the scans on your local machine. You should scan with multiple programs because no single program is 100%, so be patient this can take hours. Quarantine anything your programs find. If the program tells you it cannot remove a file, write down the name and location of the file and delete it manually.

    - How to boot into safe mode

5. Next, try booting your machine into **Safe Mode with Networking** (if available with your operating system) and run the online virus scans we listed above; remove anything they find. If Safe Mode with Networking is not available, you should still try to run them with a Normal boot to the operating system. If the program tells you it cannot remove a file, write down the name and location of the file and delete it manually.

    - How to boot into safe mode

6. If you are still having trouble:

    - It may be time to post on a computer forum or see your local (trusted) computer dealer, especially if you have not backed up your data, email, photos, etc.
    - If you are going to a computer shop, make sure you tell them you do not want to lose your data! Some places will just format the drive and you will lose everything.
    - If you do not care about losing everything, you can save money and format the drive yourself, reinstall all your programs, and download all of the updates again. This is time consuming and takes many hours to complete, depending on the number of programs you need/want to reinstalled, and the amount of backed up data you have.

7. When posting to a computer forum, it's helpful if you list exactly what steps you took, along with additional information that may be useful in solving your problem (e.g. the operating system you're using, the antivirus programs you scanned with, any errors that may have appeared, etc.). This helps prevent repeating steps you have already taken and usually speeds up finding a solution.

    When dealing with viruses and spyware, it is helpful to see what is running on your computer. The easiest way for you to show this is to post a HiJackThis log. Some forums may ask you to post this information so they can get a better idea of what steps you should take. HiJackThis is a free utility which quickly scans your computer to find settings that may have been changed by

spyware, malware or other unwanted programs. It then creates a report, or log file, with the results of the scan which you can upload or post to the forum.

You can download HiJackThis from the first link below. We have also included a second link to a guide explaining how to use HiJackThis and how to read the log that is generated.

- HiJackThis
- How to Use HiJackThis

SAFE SURFING

We have discussed how to keep yourself safe, which we prefaced with "nothing is 100%," so let's cover some items to consider about configuration and protecting you from your, or your child's, bad surfing habits.

- Have only one account on the computer with administrator rights, and use it only when installing new programs or running antivirus or antispyware scans.
- **NEVER** use Limewire, Ares, Kazaa, Incredimail, BitTorrent, UTorrent, Azureus, Bearshare, or any other Peer-To-Peer (P2P) applications! **EVER**!!! We cannot stress this enough, it just opens you to attacks. Buy your music, porn, or any other copyrighted material at a store. You will avoid putting a hole in your firewall, fines, identity theft, and downtime.
- If you think you're getting a deal that's too good to be true, well it is, and don't do it.
- Forwarding that email to 15 friends in the next ten minutes will not make your wishes come true, make you rich, or have the person you really like call you and fall in love with you in the next few minutes. People find it annoying to receive these emails, and it can be a threat if the email is infected. Do yourself and everyone else a favor, do not open or forward these emails, just delete them.
- If you receive an email from your Bank, Credit Card Company, etc. claiming they have lost your personal information and need you to reenter it, do **NOT** use the link in the email until you confirm the email is legit! Call the company and give them the information over the phone, or confirm they sent the email.
- Before you play games online, check out their credibility with a search.
- Remember, just because you have a home firewall does not mean it will stop requests you make. If you ask for it, you will get it, whether it is good or bad.
- Protect yourself and your kids. Use the parental controls in Vista, security suites parental controls, or third party software like K9 web protection. If you are unsure how to use them call your vendor; it will be worth the time.

LEARNING LINKS

From Linksys

- Networking Basics
- Home Network Security
- Video Tutorials