Securing Your Windows PC

This guide will be on securing your Windows computer from local and remote attacks by using certain security features that come with Windows to protect your information as well as the use of software to help protect your computer from unauthorized access by intruders. It will also deal with personal privacy and how to keep your important information from getting in the hands of others. Hopefully, when you are done reading this you will have a better idea on what should be done to keep your PC and your personal information from being exploited by curious or malicious users.

Securing Your Windows PC / by Resolution 2/10/02

1.1 Introduction

We all know that Windows is horrible when it comes to security. After years of constant bugs and vulnerabilities due to bad coding, many people have grown to dislike Microsoft and its little Windows operating system. So this article will be on the subject of securing your Windows box in an attempt to help you feel more at ease when using the buggy little Microsoft product. In it you will learn how to secure your system from the most common local and remote exploitation. In no way am I saying you should follow every one of these methods, just the ones that you feel would be accustomed to your needs. I will try not to get to technical with this so if I leave something out chances are I did it on purpose. With the different subtopics, it would be easy to go into great detail on either one of them but I will try not to get too technical and just stick with the basics. This article is divided into two main parts: “Privacy and Local Security” and “Remote Security”. I have a feeling this paper will be a nice size one so let’s get on with it shall we.

2.1 Privacy and Local Security

2.2 User Mentality

In my opinion, the most important form of security is you. You have to understand that no matter how much software or hardware you add to your computer or how many tweaks you apply to your system, you will never be 100% secure. The next best thing to do is to see how close you can get to that 100% comfort zone of security. So I say it all starts with you, the user. If you don’t have the mentality or mind set to secure or update your system, then that can be one of the most dangerous types of vulnerabilities there is.

Also, never let someone else use your computer if you don’t fully trust him or her. If you don’t really trust the person and they want to use your computer, make sure you watch them closely while they are on it. You don’t want someone searching for, copying, deleting, or installing something onto your hard drive.

2.3 Cookies

A cookie, in computer terms, is a small text file placed on your computer by a web server to tell that web server that you have returned to that particular web page and sometimes they can be used to track your movement not only when you return to the site, but when you surf, or exit that particular website and only that website as well. It is like your personal identification card that can only be read by the web server that gave it to you. They are normally kept in a file called “Cookies” in your windows directory.

Cookies are basically harmless but can be used by a site to get a certain profile about your web surfing habits and interests. They can also be used by sites to remember information such as your email, phone numbers, and home addresses if you had filled out any online registration or order forms on that particular site before. That information can also be given to affiliates of that site so that other sites would know your surfing habits and your personal interests in certain subjects. Now, this isn’t really a security issue but it is a privacy issue that most paranoid people might not want to deal with. So, its not really necessary, but if your paranoid and want cookies on your machine to be disabled you can view the following…

Enable/disable the cookies in Internet Explorer 5.x:

1. Go to ‘Tools’ at the top menu, and then click ‘Internet Options’.
2. Select the ‘Security Tab’ then click the ‘Custom Level’ button.
3. Scroll down to ‘Cookies’ and then choose an option of security.

Enable/disable the cookies in Internet Explorer 4.x:

1. Go to the ‘View’ menu at the top and then click ‘Internet Options’.
2. Go to the ‘Advanced’ tab.
3. Scroll down to ‘Security’ and then ‘Cookies’.
4. Scroll down to ‘Cookies’ and then choose an option of security.

Enable/disable the cookies in Netscape 4.x:

1. Go to the ‘Edit’ menu at the top and then click ‘Preferences.
2. Scroll down to ‘Advanced’.
3. In the ‘Cookies’ options, choose an option of security.

If you disable cookies, the remaining cookies that are still on your browser will still be functional with Internet Explorer and Netscape. If you disable cookies then you should delete all the cookie .txt files from the directory C:\WINDOWS\Cookies

2.4 Spyware

Spyware, also known as “adware”, is a program that is downloaded without the user’s knowledge when he/she downloads certain types of free programs from the Internet. The spyware application runs in the background of the user’s computer without the user ever knowing it has been downloaded. Spyware applications are created by the software authors to make money from the product you downloaded through advertisements. Spyware contacts its server constantly while you are on the internet, literally turning your computer into a small server, sending its own server information about you which can be anything from the sites you search, to information about your computer, to personal information such as your email addresses, home addresses, phone numbers, or possibly your credit card numbers. Sounds illegal doesn’t it? Well, its not. To many privacy advocates out there, it should be. Hopefully, the debate over spyware will end with it being illegal but until then, be careful what you download.

Now, let’s not panic. Spyware isn’t in all freeware programs you download, just certain ones, so don’t say you won’t download anything free ever again just yet. I will name some popular programs that contain spyware in them at the end of this article. However, there are anti-spyware programs for you to download that will find and remove spyware programs from your computer. One of the best spyware removal programs is called Ad-aware, which can be found at http://www.lavasoftusa.com/aaw.html. If you want, you can run a search for other spyware removal programs located at http://download.cnet.com/.

2.6 Password Security

Passwords are used by millions of people everyday when dealing with computers or Internet related security for some type of user account login. Unfortunately for some, a lot of people tend to use fairly weak or easily cracked passwords when they are asked to enter one for security reasons. Here is a small list of what lazy or non-security conscious people would enter for their passwords. This is a list of what NOT to do…

1. The user might enter his/her name, birth date, or something of great interest as a password.
2. The user might enter a relative’s name, a phone number, social security number.
3. The user might enter the word “password”.
4. The user might enter a password like “123456” or “abcdef” or “qwerty”.
5. In some instances a user might not have a password entered at all.
6. Any password shorter than 6 characters
7. Any password consisting of a word that can be found in any dictionary, in any language.

A strong password, on the other hand, would give the person who is attempting to crack your password a much harder time in doing so. The cracker might spend long amounts of time or maybe not even get the password cracked at all due to factors such as the password cracker’s limited amount of word possibilities in the dictionary list, limited amount of techniques the password cracker has to cracking the password, or the amount of patience the cracker has. Here is a list of traits that a good, strong password would have…

1. A strong password would consist of random letters, numbers, and special characters that don’t form a word or name that can be located in any dictionary, foreign or domestic. The password should have one special character within the first 5 characters.

2. A strong password should be more than 7 characters long.

3. A strong password should be easy to remember. A person can remember passwords easily by turning the password into an acronym (i.e. The password m1p!$uF@k could be remembered as “my leet pass is so unbreakable for any cracker”). Well you get the idea. Make up your own and if your data is really sensitive, make the pass up to 16 characters if you want or as many maximum characters as you are limited to.

A much more informative look at windows password security can be found at here

So we all know what and what not to do when we create strong passwords but where does Windows store those passwords whenever you make a saved user account or tell the computer to save a password so you won’t have to retype it? Well, in Windows 9x, your usernames and passwords are stored in .pwl files (password list) while in WindowsNT/2000, your usernames and passwords are stored in a SAM (System Account Manager) database file.

Pwl File - Normally found in the directory C:\Windows, a .pwl file is where Windows 95/98 stores all of its cached (hidden) password information. This serves useful for the user of the computer in that he/she doesn’t have to retype a password each time they access a passworded resource. The problem with .pwl files is that they are not secure and are vulnerable to local .pwl file cracking attacks. Windows 9x computers were not built with security in mind so anyone who has local access to someone else’s Windows 9x computer can easily crack or decrypt the pwl file and gain access to the passwords while the computer is unattended.

SAM File – Normally found in the directory C:\Winnt\System32\Config\Sam, the SAM database serves the same purpose as the .pwl file on Windows 9x distros in that it holds all of the usernames and passwords in encrypted form. The SAM database is much more secure than the pwl files in that it uses a one-way encryption algorithm or hash to secure its information. This means that while Windows NT/2000 is running, a user can’t access the SAM file from Windows Explorer because it is locked. Not a bad security feature actually. Only problem is the SAM file is still vulnerable in a couple of ways such as booting from a DOS floppy to copy the SAM contents and crack them on another computer, or to use popular tools such as L0phtCrack, NTCrack, or Pwdump to extract the hashes from the registry. To secure your SAM file and greatly reduce the success rate of these tools you can use a tool that was first produced for Windows NT in its Service Pack 3 called SYSKEY. SYSKEY was created to protect the user account data contained in the SAM registry database with a 128-bit encryption key. SYSKEY is optional with Windows NT but with Windows 2000 it comes already turned on. To activate it on NT systems go to Start, Run, and type in…

```
C:\WINNT\system32\Syskey.exe
```

Before you do you should read a little more about it since it can’t be deactivated. For more information on SYSKEY go to http://www.cert.org/security-improvement/implementations/i028.02.html

On a side note, most instant messenger programs and email accounts (most accounts in general for that matter) have an option to save your passwords on them so you won’t have to retype them or forget them next time you sign on. Never use this option when you are on a computer that is open to the public or other users. The passwords can easily be retrieved from the pwl or SAM files in Windows. There are also tools that let you view Windows passwords (including instant messengers) by viewing the passwords when they are present as only (*****) asterisks. So be cautious when using the save password feature.

2.5 Setting Windows Login

This is a login I'm sure many of you have seen before in libraries or on school computers. It's the login that pops up whenever you start up your computer and it asks for a username and password. This is a useful little feature that can prevent the average human being from entering your desktop. To set the Windows login feature, view the following…

Enabling Windows Login in Windows 9x:

1. Go to Start, then Settings, then press Control Panel.
2. Double click the Passwords icon.
3. Press Change Windows Password in the password properties window.
4. Type in your new password and confirm it by typing it in again.
5. Press OK, then press Ok again, and then reboot the computer.

Enabling Windows Login in Windows NT:

1. Press Ctrl + Alt + Delete and then click Change Password.
2. Type in your new password and confirm it by typing it again.
3. Press OK, and then press Ok again.
4. Once you are back to the Windows NT Security dialog box, hit the ESC key, which will take you back to the Windows NT desktop.
5. Reboot the computer.

On Windows 9x machines, the login can easily be bypassed by pressing ESC when it comes up. You will then be taken to the desktop. Not really a good form of security but it could keep someone who isn't familiar with Windows security from accessing the desktop.

2.7 Screen Saver Password

The screen saver password can be a useful security measure if you happen to leave your desk/cubicle at work or even at your home (depending if you have a nosey family or your just real paranoid). When you leave the computer unattended to, your screen saver will pop up during a set amount of time. To get back to the desktop you would have to enter a password. This can be useful for discouraging unauthorized snoopers while you are away from your computer unless they reboot your system, which will take you back to the desktop if no Windows login is present. So you're saying to yourself, "Well what kind of security is that? All they have to do is restart the stupid computer." True, but remember, this is Windows we are talking about and security isn't what they are known for. Also, if you are snooping on someone else's computer, you want to get on and get off as fast as you can. The intruder would have to take into affect how much time it would take for the owner of the computer to get back to the desk, the allotted time it takes to restart the computer, if the computer has a login (assuming he/she doesn't know about the ESC bypass on Windows 9x distros), and the suspicion, by the owner, of the closed applications or programs that were left running on the desktop (if any). All of that, combined with some nervousness, would add to the security part of the screen saver password in my opinion.

Enabling the Screen Saver Password in Windows 9x:

1. Right click on the desktop and go to Properties.

2. Go to the Screen Saver tab, check the box marked Password Protected, then press Change.

3. Enter your password, confirm your password, then press Ok, then click Apply, then press Ok.

2.8 File and Print Sharing

File and print sharing is an option that is part of the windows networking which enables a user to share files an printers with any person over a network or over the internet. When this option is turned on, the port 139 opens on your computer (I'll get more into ports a little later). This is the port in which file and print sharing takes place on. Though this port serves a valuable purpose, it is also one of the most dangerous ports there is and the port that most hacks occur on.

Malicious hackers love this port because it is very easy to gain entry to another person's Windows computer when the file and print sharing option is activated without a password protecting it. If you are not using file and print sharing for anything then I strongly urge you to make sure it is disabled in the networking options. If you are on a connection that is online 24/7, such as cable or DSL, and file and print sharing is enabled without your knowledge and your system has no firewall, then sooner or later you will be hacked. Here are some directions on where to go so that you can check and see if file and print sharing is disabled…

To enable/disable file and print sharing on Windows 9x:

1. Go to Start, and then to Settings, then press Control Panel.
2. Double click on the Network icon.
3. In the Network window that pops up click File and Print Sharing at the bottom.
4. Make sure both boxes are de-selected then press OK, then Ok again.
5. Reboot your computer only if the boxes were checked.

To enable/disable file and print sharing on Windows NT/2000:

1. Go to Start, and then to Settings, then press Control Panel.
2. (Windows 2000 Only) Double click Administrative Tools.
3. Double click Services, then Server.
4. Select Disabled for Startup Type, then click Apply, then OK.

2.9 File Security

Ever had some files on your computer that were very important and you just wanted to keep them safe or out of reach from your curious family members? Did you ever have a file that you wanted to make sure was practically unrecoverable from your computer? Well, securing your data can be very useful when you are on a computer that someone else has or could have access to. You don't want some stranger roaming through or editing your files while your gone. Providing yourself with this type of file protection can be done in a few ways.

Every Windows file has certain attributes that give the operating system or software information on how the file is to be used. These attributes themselves can give the files their own type of security. When you right click on a file and go to "properties" you will notice at the bottom that the file has certain attributes named Read-only, Archive, Hidden, and System. When selected, these options perform the following functions:

Read-only- when this option is checked, the file will be readable but unable to be modified.

Archive- this option indicates that the file has been changed or edited since it was last backed up.
Hidden- this option means the file is hidden from normal directory searching.
System- system files are normally used by the OS. Do not edit or delete them unless you are advanced.

Out of these four options a person would most likely use “read-only” and “hidden” to secure their files. If you set a file as read-only, it would remind a user who is attempting to edit the file that the file isn’t meant to be changed. Now I know this isn’t a type of maximum security, unless you are computer illiterate and don’t know how to turn the read-only option off, but it would help in reminding a non-mischievous person to “do not touch”. The “hidden” option can be more useful in that it can be used to hide your entire file from anyone doing a file search on Windows Explorer (not Internet Explorer) or DOS “dir” search. Once your file is hidden, you can access it by going into the directory that you placed it in by using the Windows Explorer address bar. Then type the path name of the hidden file (i.e. C:\Windows\Hidden_File). Another way is to go into the Tools options at the top of Windows Explorer, then down to Folder Options, then click on the View tab, then look in the Advanced Settings box, then check Show All Files, then press Ok. You can set the option back to Do Not Show Hidden or System Files when you have found your file. In DOS, to show hidden files all you have to do is type the command “dir /A”.

Another way to secure your files is to encrypt or password protect your files. The files themselves do not come with a pass wording function but you can secure your files by pass wording Windows like shown before or you can do it with the help of third-party software such as WinZip. I think the vast majority of Windows users use the program WinZip so I will use this as an example and give the names of other potential pass wording programs as well as file encryption programs afterward.

To protect your files using WinZip you first have to zip it. Simple enough. What a zip file does is take multiple files (or one single) and compresses them into one single zip file ending in the extension “.zip”. Let’s say you have a file that you want to keep private by pass wording it with WinZip.

Enabling the WinZip password protection:
1. Find your file. Right click on it and press “Add to Zip”.
2. (multiple files only) Find the folder that your files are in. Right click on it and press “Add to Zip”.
3. Once the WinZip window appears press “I agree”. At the bottom right hand corner click “Password”.
4. Enter your password then re-enter it. Press Ok.
5. Set the correct path that you want the zip file to be stored in. Press Add. Exit WinZip.
6. Find the location of the file you zipped it to and to unzip it you will need your password.

Remember, if its real sensitive information you can add lots of characters to your password scheme along with using the strong encryption method shown earlier. Now I won’t lie to you, there are WinZip password crackers out there capable of breaking your pass. Although, I counted a maximum of 100 possible characters you can add as your password in WinZip. If strong encryption was added to that, that would be a hell of a password. So if you have sensitive information make sure it’s a lengthy password of over 10 characters and set the zip file as a “hidden” file like we discussed before.

To find other software titles that will help you password or encrypt your files you can search the following websites:

Download.com
ZDNet Downloads
Tucows
DaveCentral

File security doesn’t have to be limited to just password protecting, encrypting, or storing your files, it can also deal with making sure your files are never retrieved after you have deleted them. Yes, that’s right, retrieval of files that have already been deleted or shall I say, “deleted”. To those of you who don’t know, once you delete a file, Windows sends that file to the recycle bin, and after you empty it from the recycling bin its still not quite gone from your system, which means important or private data that you didn’t want anyone to see can still be recovered.

In Windows, there is a (FAT), or File Allocation Table. This table keeps track of where the files are on your hard drive. When a file is written, it is stored in different clusters that may be scattered all over your hard drive. What the FAT does is keep track of the order each cluster is in and where it is located. Windows will then reassemble the clusters into a complete file and places it wherever you want it to be read. So when a person deletes a file from the recycle bin, they are only deleting its entry from the FAT. The file itself still stays on the hard drive until it is overwritten by new data. Anyone who knows where to look can find this supposedly deleted data by using certain data recovery programs such as here

This final section on file security is for the utterly paranoid or anyone who wishes to sell his/her old computer, but wants to make sure the hard drive is free from any information that might be a threat to your personal privacy or your security. This section is on “disk wiping” (which is also sometimes called file shredding). Disk wiping is almost like file shredding except it has nothing to do with tearing up a file before it is deleted. It deals with overwriting all data on the hard drive itself and making sure old, deleted data cannot be recovered.

Disk wiping (as well as file shredding) uses the following deletion algorithms to secure a hard drive:

Single Pass – The data area is overwritten once with 0’s, 1’s, or pseudorandom data.

DoD Method – The standard approved by the Department of Defense in which the data area is overwritten with 0’s, then 1’s, then pseudorandom data (alternatively once or more than 3 or more times. The data standard for this can be found in section '8-306. Maintenance' of the Department of Defense manual which can be found here. The manual basically gives instructions on how to totally overwrite data by cleaning and sanitizing it on magnetic tape, magnetic disk, optical disk, memory, equipment, and printers, making sure the data is completely sanitized or destroyed. If you are planning on getting rid of any of your components on your computer that may hold data you should read it because it’s quite interesting and informative.

Guttman Method – a very secure method that overwrites the data area 35 times.

NSA erasure algorithm – NSA approved method of deletion in which a seven-pass overwrite is used on the data area.

Disk wiping overwrites by layers. What this means is you have a surface of data clusters that still may contain file information until something overwrites it. When I say that 0’s and 1’s are used, I mean that a layer of 0’s (or nulls) are stacked onto the data area, then a layer of 1’s are stacked onto the 0’s, then a layer of 0’s are stacked onto the 1’s, and so on depending on how many passes you plan on making and what overwrite method you plan on using. After that, a layer of pseudorandom data is stacked on top of the 0’s and 1’s. Obviously, the more you overwrite data, the less likely it will be for anyone to recover it.

One of the better disk wiping utilities you can use are Eraser, CyberScrub, and BCWipe. If you don’t care to spend any money, you can attempt to search for ones that are free on the download sites I showed you earlier.

I have to also recommend a paper called Secure Deletion of Data from Magnetic and Solid-State Memory by Peter Guttman, for anyone who wishes to learn more on the subject.

2.10 Windows Update

Every so often, Microsoft will find vulnerabilities in its Windows software and create patches or fixes for the problem. At the same time, they also will create upgrades and software components that can help your computer to run better. They make these components available to their consumers by adding them to a part of their website called Windows Update. It is recommended and sometimes necessary that all Windows users visit the Windows Update site on a regular basis. Most Windows users can find an icon link to the site by pressing Start, then scrolling your mouse pointer up to the top of the Start menu and looking for an icon that has “Windows Update” next to it. If you don’t have it then you can go visit the site by clicking here.

3.1 Remote Security

3.2 Port Numbers

In dealing with remote security over the Internet, we come to what’s called port numbers. These are, in Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), a series of numerically assigned ports, which are used to connect a client or send data to and/or from a client to a server through different yet specific processes or services running on each port. For example, if a home computer wanted to connect with a university server through telnet, it would have to connect to port 23 of the university server, which is the default telnet port. If a client wanted to connect to a server via File Transfer Protocol (FTP) (port 21) to transfer files, the client would have to send a request to the server in which the server would verify which port the request is asking for and then connect the client to the requested port, which is port 21 of the university server.

The Internet Assigned Numbers Authority (IANA) holds a list of port numbers, their protocol, and what processes are running on them. If you wish to see the list, you can go here.

3.3 Firewalls

Firewalls are programs, which protect the resources of a private network from unauthorized entry by users of another network. All data flowing in and out of a network or your computer goes through the firewall. They can be both hardware and software and are used to block and regulate what data is acceptable and not acceptable for access through the ports of a computer network.

Some firewalls are made for packet filtering, which means they filter out what packets (data messages) are allowed to go through the firewall depending on a set of rules created by the user. Other firewalls, more notably called proxy servers, sit between you (or a network) and the Internet and filter all information through the proxy (also providing caching) along with providing protection for the LAN (Local Area Network) or your computer by hiding the computer’s Internet address from outsiders.

So why should you get a firewall anyway? Well, for one, you can go on the Internet and download really good ones now for home use for free! So now you don’t have any excuses not to get one to protect your computer while online. It also doesn’t matter what type of connection you have since a firewall can be used on anything from a slow 28.8k modem to the highest speeds available. Another reason is obviously for security. Unfortunately, the Internet has people on it who think they can do whatever they want without getting caught. These people like to go around and tamper with or break into other people’s computer systems. On Windows systems, port 139 (Netbios/file sharing port) is the main target by attackers who want to use programs to flood a connection offline or break into a computer if file sharing is turned on. A firewall is the first line of defense to stop these idiots from penetrating your system.

A firewall is a must for users of cable or DSL connections since these connections stay online 24/7 and are the most likely to be the main target of a computer break-in. Most cable and DSL connections also have a static IP addresses, which means your computer’s Internet address is always the same when you are online and never changes like a dynamic IP would. This means that the attacker would be able to find your computer online any day of the week if he/she felt that your computer was exploitable. Firewalls can add to the security of your computer greatly while online or on a network in that they will help block the ports that these attackers are trying to gain access to or exploit. Also, almost all of them come with logging capabilities that will log (by date, time, month, connection type, type of attack, attacker’s computer address, etc) anyone attempting to access the ports on your computer.

So you’re not sure which firewall to get but you would like one that is affordable, user friendly, and one of the best? Well I picked two of the free ones that I’ve tried and also the ones that seem to be the most popular…

Tiny Firewall 2.0.15 – A personal favorite of mine, which is why I use it. It is a free firewall that is easy to install and comes with local and remote administration access as well as logging capabilities. Easy/novice understanding of its configuration is needed. Advanced features include the ability to edit, add, and delete filter rules for one port, multiple ports, or a specific remote IP address/range. For more information on Tiny Firewall, including an online manual, visit its website at http://www.tinysoftware.com.

Zone Alarm 2.6 – Zone Alarm is a free firewall, which extracts itself when you download it for easy installation. It’s made for people with little knowledge of networking. Zone Alarm comes with a configuration that’s real easy to understand and easy to configure. Two gauges on the side monitor incoming and outgoing activity. Logging includes a “Whois” function to identify unauthorized intruders. Has a stealth mode that makes your connection seem invisible to outsiders while online. A drawback is that it comes with some spyware that you can remove quickly by downloading the free program Ad-aware to fix that problem. For more information on Zone Alarm visit its website at http://www.zonealarm.com.

Here is something that a lot of people don’t understand and are quick to panic about. Once you download a firewall, you might wonder why it is warning you that your ports are being probed. You might even think your being hacked. Well, chances are your not. The odds of someone deliberately hacking your computer for personal reasons are very slim. For someone online to exploit a computer, they need to find one that is vulnerable. Searching for a vulnerable computer on the Internet one by one is extremely tedious. So instead of searching one by one, attackers will use port scanners to scan a wide range of computers for vulnerable ports (the main one on a Windows computer is always port 139). You may think at first that its just your computer that is being scanned when in actuality, the port scanner just skimmed over your ports (since it saw your ports were protected by a firewall) and moved on to the next computer in what could be a series of thousands of other computers waiting to be scanned on the net. If your firewall is alerting you constantly about this then you should lower your security settings if you don't wish to be bothered.

3.3 Viruses

A virus is an artificial or man-made code or program that is made to secretly infect or attach itself to one's computer by infecting executable files and important system files on your hard drive by replicating or copying itself which can use up your computer's memory. Generally they are harmless but can also be a danger to the files on your computer depending on what they were programmed for.

Not all viruses are the same and only do the tasks that they were programmed to do. There are viruses that are only programmed to infect program files for the sole purpose of damaging them or interfering with the computer's operations. Some viruses, called macro viruses, are programmed to infect applications such as Microsoft Word or Excel, executing itself each time the application is opened. Other viruses can infect the boot sector of floppy disk and hard drives which means that if the boot sector of a hard drive is infected then any floppy you put in it will be infected and if the boot sector of a floppy is infected then the floppy can infect the computer that you inserted the floppy into. Viruses called multipartite infect both the boot sectors of hard drives and floppies as well as program files. So how does one's computer become infected with these viruses? Here are a few ways…

Common ways to catch a computer virus:

1. Through the exchange or use of infected floppy disks, CDs, Zip disks. Even if these items are brand-new are come straight from a trusted friend, they can still be unknowingly infected.

2. Downloading infected files from the Internet, especially third-party vendors. (If your going to download anything off the internet, make sure the website is trustworthy and reputable)

3. Through email attachments. (Make sure you scan the file with a virus scanner first before you open an attachment)

4. Be careful of double file extensions like "Poems.txt.exe" that are made to trick a person into thinking they are downloading a text file when they are really downloading a virus program.

5. Through file transfers while in chat sessions and instant messenger chats. (Never except strange downloads from a stranger, especially ones that end in .exe, .sys, .vbs, .zip)

Remember, a virus can only infect your computer if you execute the file that it comes in. This means that even if you download a file that contains a virus, you aren't infected yet. You will only be infected if you execute the file (double-click it). This is why they say you should scan a file first with a virus scanner before you open it. If you scan the file and your virus scanner shows that the file is infected, just delete the file or in some cases, your virus scanner will put it in quarantine for you (more on virus scanners in a bit).

So that was common ways on getting infected with a virus. Hopefully this next bit will make even less paranoid of viruses. Here are a few things that viruses cannot do…

Common virus misconceptions:

1. Viruses absolutely cannot harm your hardware or physical computer components. They can only harm the data inside. Also, a virus cannot blow up your processor

or monitor, so for all you rookies, this is real life, not the movies, let’s not get crazy.

2. You cannot get a virus from reading your email. You would need to execute an infected attachment to catch a virus. (Hotmail and Yahoo mail both run virus scans on attachments first before you can download the file.)

3. Computer viruses cannot run on your system until they are executed.

4. You can still get viruses from disks and CDs even if they are brand new so don’t think that just because you just bought it, doesn’t mean it won’t contain a virus.

5. Viruses are not alive. (Yes, some people actually believe or question this. *sigh*) They are only programs doing what they were programmed to do.

So now the next question is, “How do I protect myself against these viruses?” For one, you can read over the steps we just went over to see how people can get infected, and secondly, you can download or buy yourself a virus scanner, which will keep watch on your computer (as long as its turned on) and warn/protect you from any files that you would receive that might contain a virus. They also can scan your system automatically (by a set schedule), and keep you informed of any knew virus definitions (list of new viruses found to scan your computer with) to make sure your system is virus free. The two top virus scanners out for Windows are Norton AntiVirus and McAfee.

It’s important to have a virus scanner on your computer since viruses are spawning faster than there are ways to stop them, even if you have to spend a little money. I guess you have to ask yourself, “How much is your data worth to you?”

3.4 Trojans

Derived from Greek legend in which the Greeks won the Trojan War by hiding in a large, hollowed out horse to gain entrance to the City of Troy, the computer version of a trojan will come off as (hidden inside of) a useful application such as a free screensaver or chat program, only to later display harmless messages, destroy files, or create a backdoor in your system for an intruder to gain access to your computer. A trojan is not a virus because it does not replicate itself.

You can get a trojan on your computer in many of the same ways you can get a virus, but one of the main purposes of the trojan is for an intruder to access your computer remotely and even control it. You do not want one of these things on your system at all. If an attacker installs a trojan on your computer by getting you to download some application, he/she can browse through your files and even your registry, format your hard drive, spy on you by viewing what you type on chats or instant messengers, spy on you through your webcam, listen to you talking through your own microphone, read your email messages, etc. Basically, just about anything you can do on your computer locally, the attacker can do remotely.

The most notorious of these trojans are Back Orifice, SubSeven, and Netbus. The Internet is filled with immature little teenage boys who think they are hacking gurus because they can trick people into downloading one of these programs that they didn’t even create so that they can gain access to others computers. Online society has dubbed these people “script kiddies” because they use tools that were created by other people for malicious attacks. They have no comprehension on how to use these trojans properly (even sometimes infecting themselves in the process), which makes them even more dangerous to your computer. So how do you know if you get infected with one? Here are a few symptoms…

Possible signs and symptoms due to trojan infections:

1. Your CD-ROM door opening and closing by itself (classic sign).
2. Messages start popping up on your monitor screen that appear to be talking to you.
3. Your printer may print out strange messages on its own.
4. Your mouse pointer may start having a life of its own.
5. An unknown person starts typing in your instant message window when you are talking to a friend.
6. Anything weird and out of the ordinary that your Windows PC does (excluding the errors, screen freezes, and blue screens of death).

If you think you have a trojan than you should turn off your computer. Once you sign on again (offline) you can find out if you have one by seeing if there are any common trojan ports open by going to the DOS prompt and type in the command “netstat –a” (without the quotes). For a list of common Windows ports that trojans run on, you can go here.

Even though trojans aren’t viruses, antivirus companies still add them to their virus definitions to prevent trojans and these people from exploiting other people’s computers without their knowledge. So it is always good to have a virus scanner running on your computer. There are also scanners designed for the sole purpose of finding and deleting trojans from your system. The Cleaner and LockDown are two good ones that you can download for a free 30-day trial.

3.5 Denial of Service Attacks

A Denial of Service (DoS) attack occurs when a malicious person(s) sends another user or server a large amount of data for the sole purpose of disconnecting the connection from the internet, slowing down or disabling their services, or crashing the remote system. DoS attacks are mainly just used to cause destruction from a single person or a group a people who wish to flood another person, websites, or servers of companies or organizations. To businesses, an attack on the company website could render the site unreachable for hours or more by its consumers which could cause the business to lose money or even damage the website servers.

A person-to-person (one person flooding another) attack would most likely occur on chat servers that support Internet Relay Chat (IRC). IRC is filled with people who like to use these attacks (called “nukes” on IRC) against others for fun, to kick people off the chat server out of anger, to harass someone, or to show others that they are “powerful”. The basic DoS attacks used on here consist of ping attacks (sending large ICMP packets to a host; also called Ping of Death) and SYN attacks.

The majority of Internet users who do use these attacks are teenage kids who don’t even know that it is illegal. Yes, that’s right boys and girls, illegal. To all those who do use DoS attacks (nukes or nukerz for the extremely lame), you should know that inflicting any harm to someone’s computer as well as tampering with it by remote flooding of any kind is illegal in the United States under the National Information Infrastructure Protection Act of 1996 and Computer Fraud and Abuse Act of 1986. If you are caught you could go to jail for a good amount of time as well as pay a hefty fine. I doubt using these attacks on people is worth all of that.

Protecting your computer from one of these attacks is not easy. People on dial-up are the easy targets since their connections are slower and more people nowadays use cable or DSL connections, which are much faster and can easily send more data to a host to slow it down, disconnect it, or crash it. The best way to protect yourself is to update your computer with the necessary patches and install a good firewall. This should protect you from a few of the attack tools that some attackers use online. For more information on the tools these attackers use and patches for them, visit http://www.irchelp.org.

3.6 Checking Your Security

A good way to see if your computer is remotely secure is to run it through security tests. You can do these checks yourself or you can do it with the help of Internet security sites. Here are a few things you can do…

1. (For people with firewalls) Use a port scanner to scan your system and see if any of your ports are visible or open. If they are then make the necessary adjustments to your firewall rulesets. Also, anyone can test their system’s security by doing a quick security check test at ShieldsUp!, HackerWhacker, and Symantec Security Check. Those who don’t have firewalls can use these tests to see just how vulnerable you are.

2. Make sure that you scan your computer for viruses every 2 weeks and also make sure your virus scanner is updated with the latest virus definitions.

3. Use the Windows Update to download any necessary system patches or upgrades.

4.1 Conclusion

Finally finished. This paper sure took up a lot of my time. I hope you liked reading this paper as much as I liked putting it together for you and hopefully you found it useful and learned something new from it at the same time. Having read this paper, you now should have a better understanding on what to do to secure your Windows PC. Always remember that your security is what you make of it, and with a little time, patience, and know-how, your Windows box can be a “hard target” for any intruder or attacker.

Securing Your Windows PC / written by Resolution (email: resolution404@yahoo.com)