A property of Know How Media

A Comprehensive Guide to Windows Security

AUTHOR : JAIBEE JOSEPH

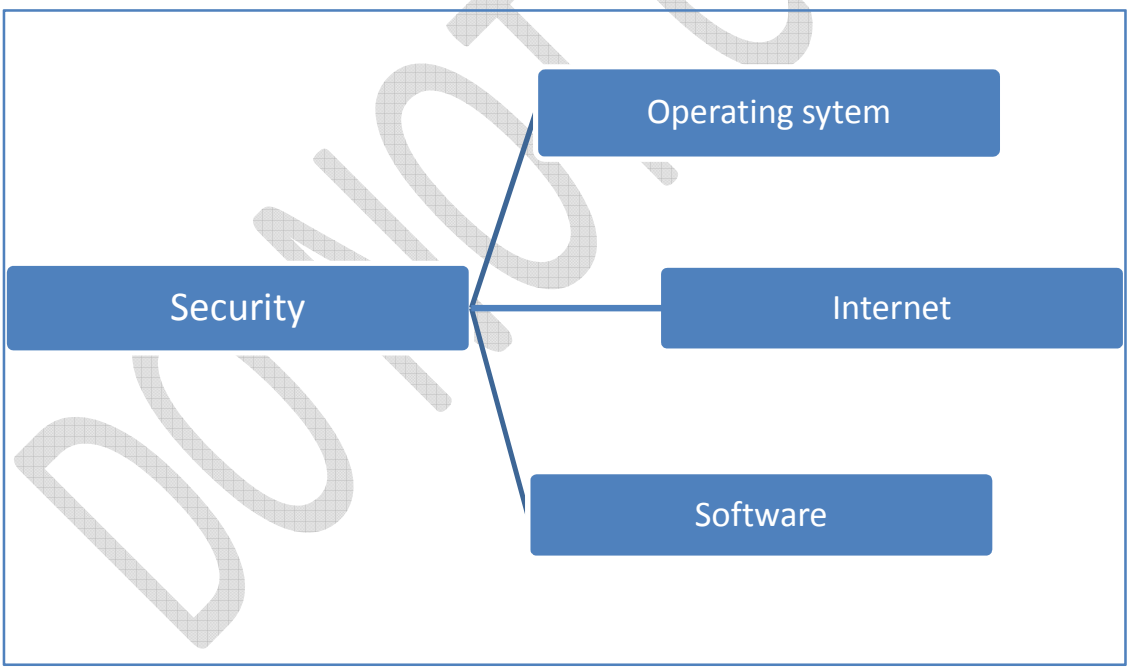
CONTACT : JAIBEE.JOSEPH@GMAIL.COM

WHY SECURITY

As computers becoming a part of our daily routine, we end up in leaving some of our sensitive information on our PC's. These starts from Password's, E-Mail Id's, Credit card numbers, online banking details etc. Then there is another risk called viruses and spyware when you are online. There is only one fundamental difference between a virus and spyware, viruses are written for destruction and spywares for gain. When we speak about computer security what it means is that, how we can prevent intruders from entering our systems.

Let's categorize the computer security in to three

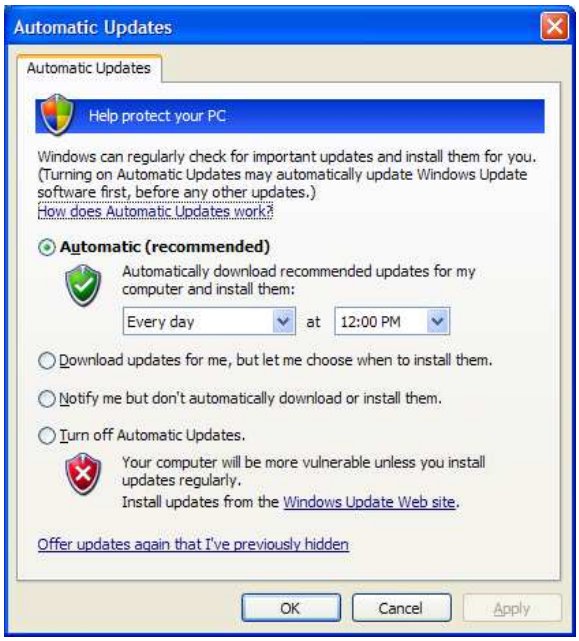
- Operating System Security
- Software Security
- Internet Security



Operating System

Operating System is that middle man that links us with the hardware. It is that unavoidable part that helps us to control the hardware the way we want. So securing the operating is an important task, because without that you cannot run your pc and your pc may become a nightmare for you if the operating system is not performing well. Here I am going to explain few ways to secure your operating system (here it is windows xp).

BEFORE ANYTHING ELSE: PATCH, PATCH, AND PATCH!



Automatic update options in Control Panel. Be sure to turn this option on to get updates from vendor to be installed automatically.

Every operating system needs to be updated, if you want it to be stable and secure. So, first step to your operating system security is to update your os. Every operating system needs to be updated to make it stable. Microsoft releases updates for vulnerabilities being detected and cop up with these updates is very important for your os security.

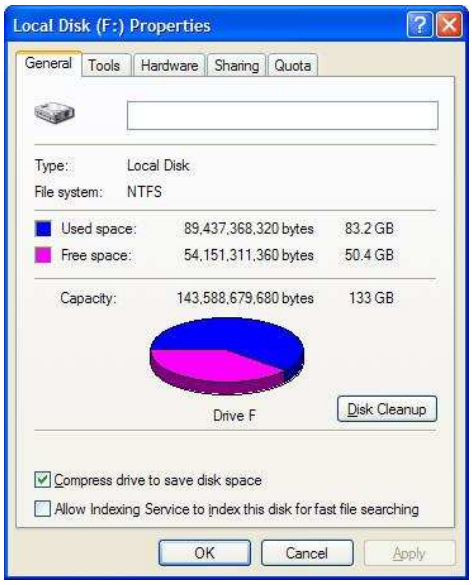
To ensure that the security update or patch is applied as soon as it is available, turn on Automatic Updates. Other than operating system updates, Automatic Updates also downloads all high-priority updates for Microsoft Office, Microsoft SQL Server, and Microsoft Exchange Server.

If your pc is offline **AutoPatcher** is a great tool for updating your system. Search for autopatcher in Google and download the latest version to update your system.

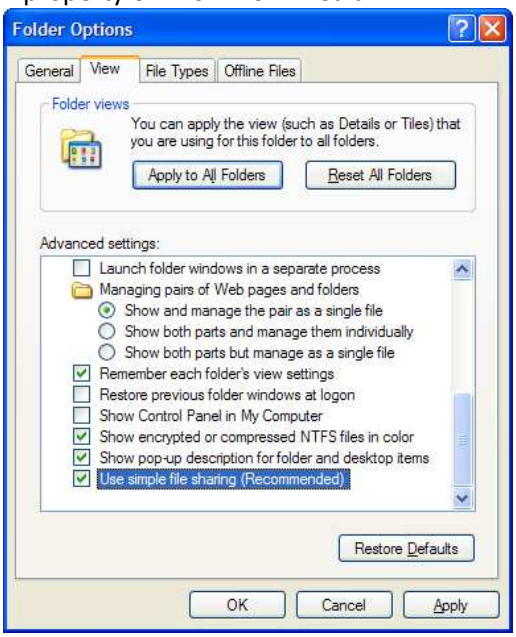
Install the latest service packs from Microsoft to ensure that your operating system is up to date. The latest SP for windows xp is SP3 and it can be freely downloaded from Microsoft's website or any other secure third party sites like www.softpedia.com .

ENSURE DISKS ARE FORMATTED WITH NTFS

NTFS is the recommended file system for Windows based operating systems. It has better access control and better security compared to the FAT file system. NTFS enables you to decide which user and which group has access to which folders and files on your system. If you have any FAT or FAT32 partitions, these can be converted to NTFS using the Convert.exe command line utility. To convert a partition to NTFS, open a command prompt. Type in "**convert drive-letter: /fs:ntfs**" (without the quotes) to convert "drive-letter" to NTFS. For example, if you want to convert drive F to NTFS, you would type in "**convert f: /fs:ntfs**".



Picture of an NTFS formatted partition in Windows XP. Make sure that the file system of your drive partition is NTFS for more security and stability. Otherwise run the above command to change the file system to NTFS.



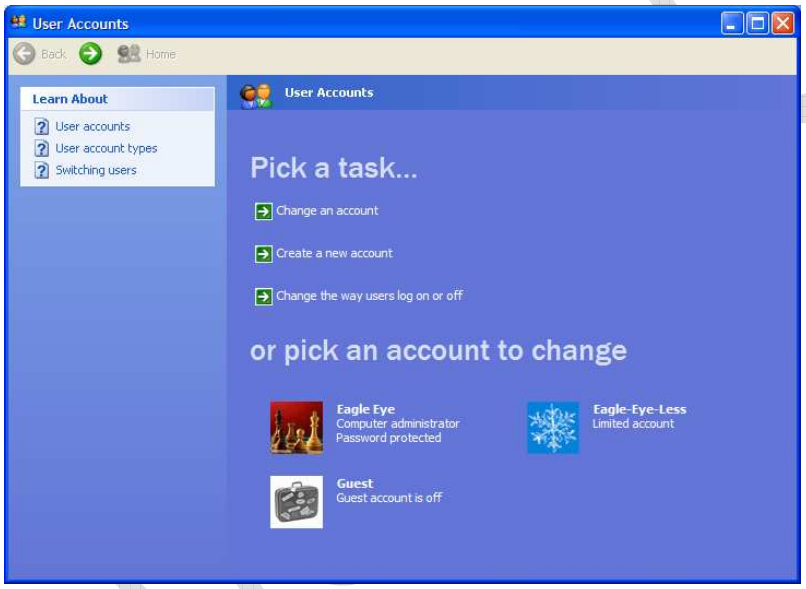
TURN OFF FILE SHARING

In a Windows XP machine which is not a part of a domain the files are shared using a feature called simple file sharing. For home PC's this option enabled may bring risks as hackers can exploit any unknown vulnerability. To turn this feature off, please follow the below explained steps:

1. Open My Computer and go to tools option.
2. Now select "Folder Options" from the menu.
3. Select the view tab from the dialog opens and move to the end of the options to find "Use simple file sharing".
4. Deselect if the option is already selected and apply the settings from the button given in the dialog.

Picture shows an xp installation with simple file sharing enabled. This feature is enabled by default in xp. Disable it for your own safety.

USE USER ACCOUNTS AND SECURE PASSWORDS



Use Windows XP user accounts manager to make sure that all your users have right privileges and power to user your system resources.

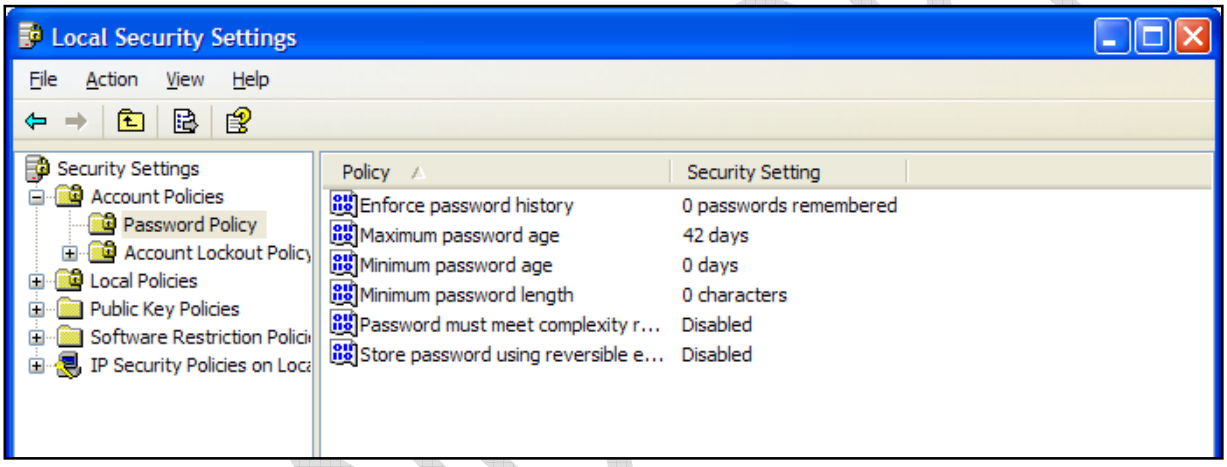
Assign passwords to all your administrative powered user accounts. It's always a good practice to use secure passwords and never to leave it blank. While you install xp, it creates a default administrative powered user account during the installation, xp asks a password for this user account during the installation and most of the users neglect this screen and continues to finish the process. When the installation is finished xp creates a new user account and the default administrator account still remains with a blank password, this may cause fatal problems if a hacker finds out the secret, that one of your administrator account does not have a password, so make it sure that you provide a strong password while the installation.

The first rule to manage user accounts properly is to provide a strong password and the second one is to use a less privileged user account while working with the internet. Running your computer in administrator mode and connecting it to the internet is a potential risk, as any malware that manages to enter the system will have full control over your system resources.

Notice: Users of a limited account cannot install software or hardware or cannot change the account name or type. For some programs it's necessary to be launched by an administrator, for such programs use the "Run As.." option to overcome the problem. Right click the application you want to run as an administrator and select the "run as" option from the menu. You will be prompted for the administrator user name and password. Provide the details and now the software is ready to go. Note that this feature only works when Secondary Logon service running, make sure that this service is running from **Control Panel > Administrative Tools > Services**

ENABLE STRONG PASSWORD POLICIES

To make sure that all your system users follow a healthy security trend, use the Local Security Policy console to setup security policies for your computer. To find this tool go to **Control Panel > Administrative Tools > Local Security Policy.**



Do follow the below parameters to set a good password security policy:

1. Make sure that the minimum password length is at least eight characters.
2. Set the minimum and maximum password age between 1 and 42. Password will expire at the end of the specified time and user will have to create a new password.
3. Set the minimum password history to 8 or more so that user does not repeat the same password.

USE ACCOUNT LOCKOUT POLICIES

In Windows XP professional edition it's possible to lock a specific user after a number of invalid logon attempts. I strongly recommend this option to be enabled as any intrusion attempt or password crack attempt can be blocked. You can find account lock out policy in Local Security Policy manager itself. Follow the recommendations below to set a good account lockout policy:

1. Set the lock out duration to 30 minutes. This will prevent the use from logging in to the system for 30 minutes after a specified number of invalid logon attempts.
2. Set the number of invalid logon attempts to 5 or 10.
3. Set the counter reset to 10 minutes.

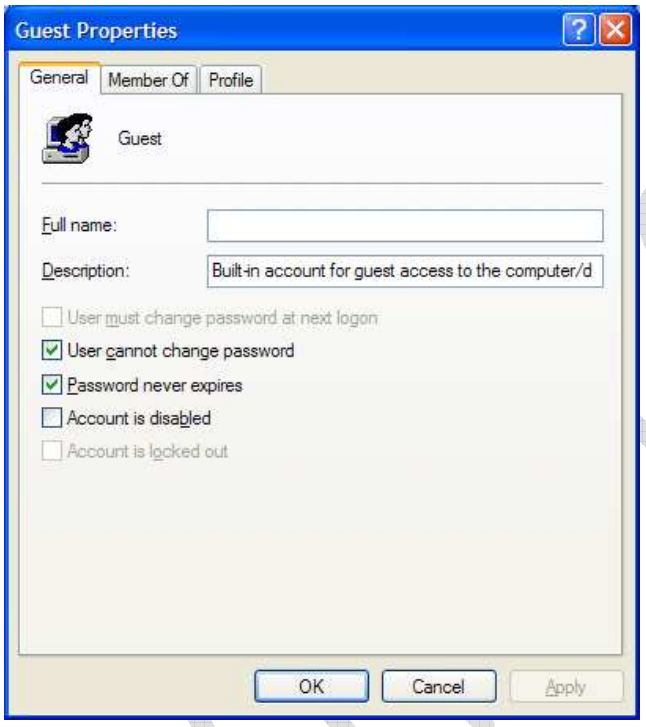
A property of Know How Media

HOW TO CREATE A STRONG PASSWORD

A strong password means better security, so be always sure that you have a very strong account password whether in the case of computer user account, internet email account or anything where a password is applied. Following are some good practices to follow while creating password

1. Never use your first name or last name as password.
2. Never use a date as a password like your birthday.
3. Never use a common word like apple or something like that.
4. Use a combination of numbers, letters and symbols to create a password eg. Ravi123$$1.
5. Never use a friends name or family mebers name as a password.
6. Atleast use a minimum of eight letters in the password.

Try to follow every rules specified above and with this you can create a very strong password which will secure your confidential information.



TURN OFF OR DISABLE THE GUEST ACCOUNT

If your computer is a standalone system that connects to the internet, you should disable/turnoff the guest account as it can allow access to your system and network shares. To disable a guest account: **Right Click On My Computer > Manage > Local Users And Groups > Users** find the guest account and right click on it and select the properties option. From the dialog opened select the option "Account is disabled" and apply the settings to disable the guest account.

Guest account properties window from the manage section of windows xp. This area is used to configure different accounts and their groups which they belongs to. Turnoff your guest account from this area for better protection.

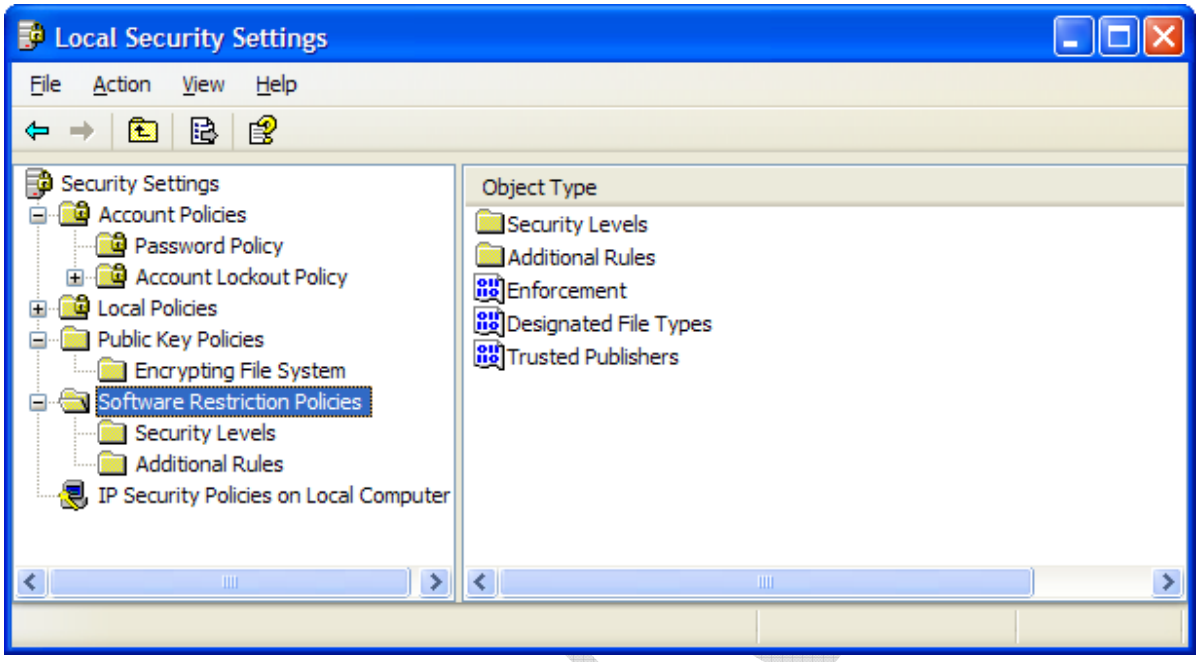
DISABLE UNNECESSARY SERVICES

When your operating system starts a number of programs start as the part of the core operating system we can call them services. Windows XP is also having a number of unnecessary or unwanted services starting with the operating system with these services comes the security risaks. So, it's very important that you disable such unwanted services. To view the services type "services.msc " at the Run prompt and press enter. Review the description of these services to get a basic understading of what it does and find the unnecessary services. Following services are typically safe to disable:

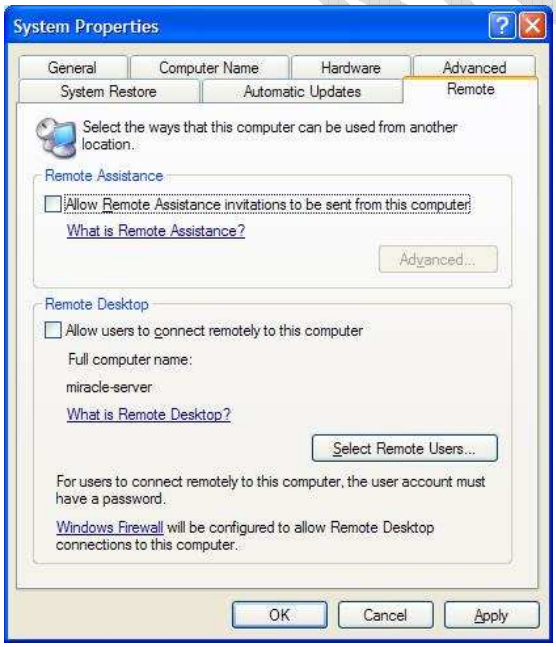
1. Telnet
2. Universal plug and play
3. IIS (not installed by default)
4. Netmeeting and remote desktop sharing
5. Remote desktop help session
6. Remote registry
7. Routing and remote access
8. SSDP discovery services

9. Wireless zero configuration (if no wireless network)
10. Background intelligent transfer service

SET SOFTWARE RESTRICATION POLICIES



Using software restriction policies you can control the software that run on your system. You can find these options from **Control Panel > Administrative Tools > Local Security Settings.** Here you can specify which programs can run of not run from your system. Any attempt from any other program without the user permission will be unsuccessful.



DISABLE REMOTE DESKTOP SUPPORT

This feature is a great way to be access all your documents while you are away from your home. But, in case you have a poor bae of security it's the best windows to your home. This feature is a very risky application to be leaved opened to the world. If you do not use a remote desktop it's a good idea to disable this feature for security reasons. Here is how..

- Right click on **my computer** and goto **properties**.
- Click on the remote tab to expose the settings.
- Uncheck the box under remote assistance and press the apply button to save the settings.

VIRUS BUSTING

In this chapter we are going to discuss about the features of viruses and how to burst them. To burst viruses you should be able to identify whether your system is attacked by a virus or not. Here are some basic symptoms with which you can identify whether your system is infected or not.

1. Your computer takes that charge and does things of its own : moving the mouse cursor all by itself, closing and opening windows automatically, showing you random messages, and so on. If any one of such things happening with you, then there is a good chance that you are infected by a virus.
2. Your computer seems to not responding to any of your commands. This symptom is mainly related to windows xp.
3. Operating system crashes and restrats continuosly is a good indication that your system is infected. Even though it can be of other reasons, in most of the cases this happens because of a high rate of virus infection.
4. Several applications seems to be not working.
5. Certain drives drives are not accessible, eventhough they showup in my computer.
6. Weird messages poups oftern is also a symtom that your system is infected. This can also be of other reasons but it depends on how randomly these messages appear and how weird they are.
7. You opened a suspicious attachment and after that everything gone out of control, then it's the time to scan your system.
8. If your antivirus is disabled and you didn't disabled it then it's highly likely to be a virus infection rather than anything else. My suggestion is that try to reinstall the antivirus software, if you find it not happening then its time to catch an expert.
9. If you are able to install any program but not an antivrius.
10. When someone tells you that he/she got a message with an attachment from you and you didn't send any message.
11. Unknown icons on your desktop.
12. Your moden is having a lot of activity eventhough you are not browsing the internet.

DETECTING AND REMOVING SPYWARE

Spyware is becoming one of the largest menace of computers in last few years. Hidden within free applications, these programs can spy on your computer activities and report home various information about your computer habits. Adware is another menace that is closely related to spyware. Just like Spyware, it can be secretly installed on your computer and will monitor what you do.Then, when the time is right, some Adware apps will display relevant advertisements.

BURSTING THEM : We've rounded up the best (and worst) of the apps dedicated to finding and killing spyware—and keeping it from getting onto your machine in the first place. Not all antispyware apps are created equal!

There are some free applications on the web that will help you to get rid of them. We recommend you two of them mainly, both created for this purpose only and focuses on Adware and Spyware. The first

application is called Ad-aware from Lavasoft. This program has a bascic version available for free which is only for personal use. The second applications is Spyboat Search and Destroy which is completely a free application.

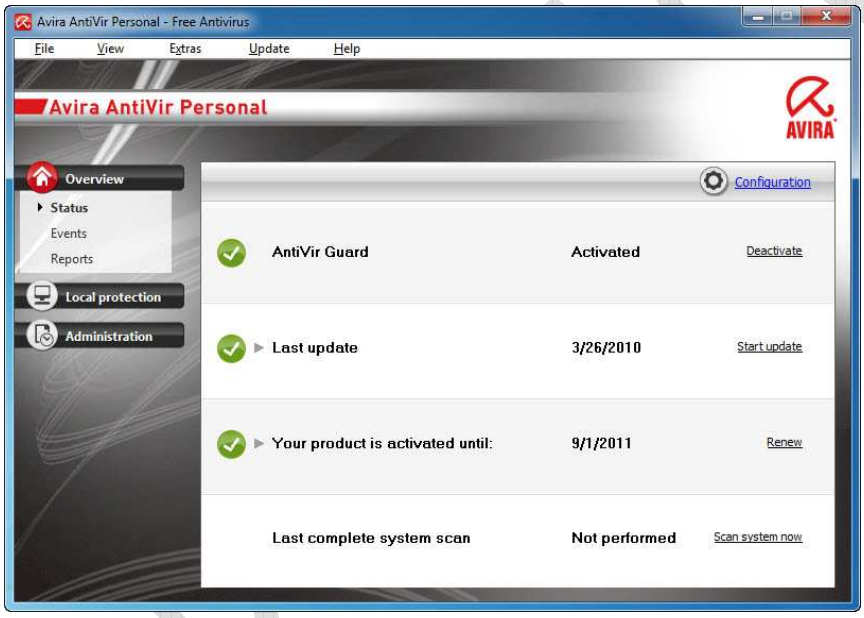
SPYBOAT SEARCH AND DESTROY : Spybot's skill at cleaning up malware-infested systems is mediocre, and it has almost no ability to protect a clean system. Spyboat still it remains to be one of the best spyware solutions out there. Spyboat provides some advanced tools which are handy for highly skilled users. Immunization prevents some problems by adjusting browser settings. Boot-time scan manages some locked files.

SOLUTION FOR VIRUSES AND HOW TO GET RID OF THEM

The main solution for any threat to a computer is obviously an antivirus. There are plenty of free and paid solutions available out there, but what matters is that, the one you chose works for you or not. Here we are going to introduce you to some of the most widely used free and paid antivirus solutions and our suggestion for you.

FREE ANTIVIRUS SOLUTIONS

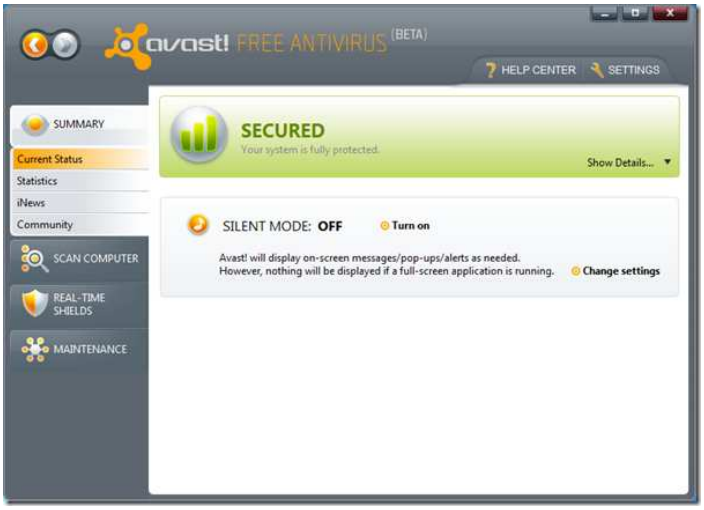
AVIRA ANTIVIR PERSONAL



Avira AntiVir Personal – FREE Antivirus is a reliable **free antivirus solution**, that constantly and rapidly scans your computer for malicious programs such as viruses, Trojans, backdoor programs, hoaxes, worms, dialers etc. Monitors every action executed by the user or the operating system and reacts promptly when a malicious program is detected.

Avira AntiVir Personal is a comprehensive, easy to use antivirus program, designed to offer reliable free of charge virus protection to home-users, for personal use only, and is not for business or commercial use.

The program is able to neutralize over 80 thousand viruses that are updated daily. Perhaps the Avira AntiVir Personal is the industry's fastest antivirus but it is lighter and effective. It works in the background without consuming too many resources or compromising the performance of the machine.

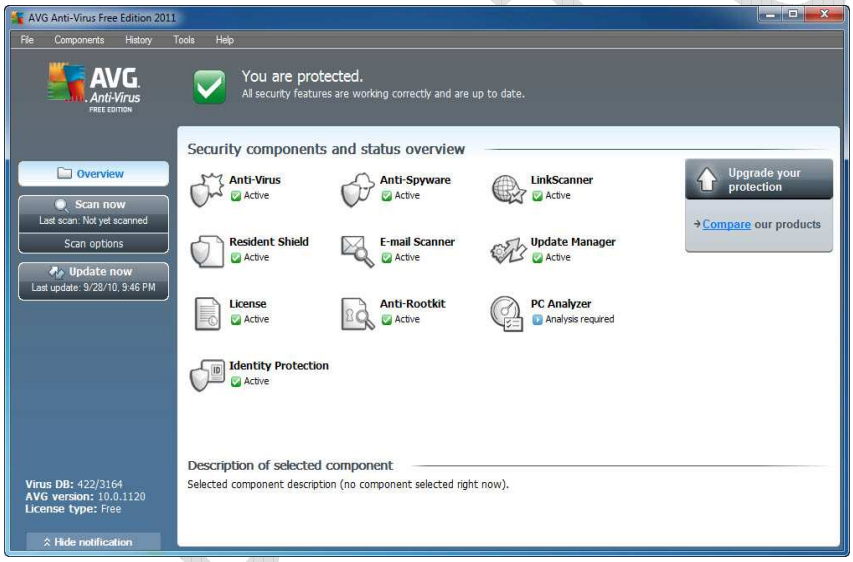


AVAST FREE EDITION

Avast! Antivirus software provides complete virus protection for your computer. Antivirus engine is complemented by anti-spyware, firewall and antispam modules to protect you against phishing schemes, identity theft and internet-distributed web viruses. Automatic updates for greater user convenience and safety. Avast is one of the top users rated among free antivirus software. Features include:

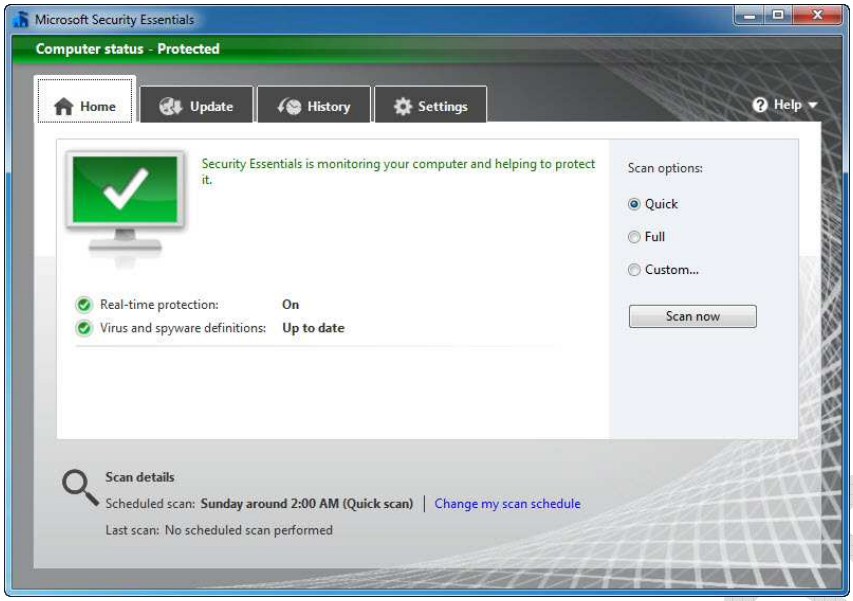
- Antivirus and anti-spyware
- Ensures all mails sent and received are clean
- Keeps you protected from “chat” infections
- Stops attacks from hijacked websites
- Compatible with Windows XP, Vista and 7
- New user interface

AVG FREE 2011



AVG with the new release is smarter, faster and lighter. AVG Anti-Virus Free 2011 is dedicated to identifying threats by behavior. Zero-Day detection was so important that something was missing. Now, with this improvement, AVG has everything to cover this gap. AVG Anti-Virus Free 2011 Interface is slightly redesigned to follow the new trends and conveys exactly what the program does. It is divided into three main areas; Overview, Scan and Update.

In overview, you know the status of each of the components such as Anti-virus, Anti-spyware, LinkScanner, Resident Shield, E-mail Scanner, Update Manager, Anti-Rootkit, PC Analyzer and Identity Protection. With a double click on each tool, you access the settings, which vary according to the resource accessed.



MICROSOFT SECURITY ESSENTIALS

Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software. Microsoft Security Essentials is a free download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology. It's easy to tell if your PC is secure — when you're green, you're good. It's that simple.

New beta version of free Antivirus from Microsoft has arrived. Compatible with Windows 7, Vista and XP, Microsoft Security Essentials is a complete Antivirus that protects your computer in real time from various threats including malware, rootkits, spyware and trojans.

Microsoft Security Essentials is a new and improved protective mechanism, because now it has advanced detection and cleaning capabilities with better performance. Now, it is integrated with Windows Firewall.

PANDA CLOUD ANTIVIRUS

Panda Cloud Antivirus is a different concept. Betting everything in lightness and extreme simplicity of use, this software is intended to protect a computer without the need to intervene and worry. It is the first and only free antivirus that brings the concept of cloud protection.

According to the developers, the protection model uses architecture composed of an agent and a server that process and block several types of malwares more efficiently than any installed Antivirus. Panda Cloud Antivirus applies technical interception of malware on the client architecture, making it possible to prevent new and unknown viruses entering into your computer through an extremely lightweight platform.

New suspect files are sent for analysis to Panda through a mechanism known as Collective Intelligence. Sent files are received by servers and are quickly analyzed. According to Panda, about 50,000 suspicions are analyzed daily.

Recommendation: Our recommendation to you out these free antiviruses is Avira Antivir Personal edition. The reason behind this selection is the fact that it has the largest virus database among the above explained and it's the lightest. Avira can be run at any system with even a little hardware configuration and now the product is now more improved and it's easily manageable by even a child.

PAID ANTIVIRUS SOLUTIONS

Here arises the question why should I pay for a solution as there are plenty of free good functioning free softwares out there? The answer is so simple, the added functionality, support and permission to use in a commercial setup.

Note: Here we would like to clear one myth existing among various antivirus users that "The Free Ones Doesn't Catch a Number of Viruses Compared to the Paid Ones". In answer to that I should say it's not a true thing; every free antiviruses and their paid version use the same engine and database for the detection purpose except some extra functionalities in the paid ones. Paid antivirus never means that it's going to catch all the viruses. You should always keep the fact in mind that it only provides some extra functionality compared to the free ones, otherwise both are the same.

Here we take a look at some of the well known paid solutions out there. It's always your choice that which one you want to use for your systems protection.

ESCAN INTERNET SECURITY 2010

eScan Internet Security from Microworld Technologies, Inc. is a complete security suite that consists all those functionalities that one paid solution should contain. Its uses a technology called MWL (Microworld WinSock Layer) which scans internet traffic in real time.

The main features that attracted us about this cool software are its detection rate and good memory usage. Its uses an astonishingly very less memory while scanning and even in real time. The detection rate found to be too good as it detected almost 99 percentage of all malware we thrown for detection to the engine. Frequent updates and free customer support are also available for the product. eScan has improved a lot in every aspect of its position in market with a great combination of look and its really works for you.

QUICK HEAL TOTAL SECURITY

Quick Heal Total Security 2010 is an Internet Security product from CAT Computing, Pune. Quick Heal offers specialized security solutions designed for personal use on individual machines for home users. These products combine high performance with exceptional ease of use and excellent design. Quick Heal Total Security gives you complete protection from viruses, spywares, and hackers. It also helps you stay connected and communicate over the internet by preventing your system from threats over the Internet. With Quick Heal Total Security in your PC - Enjoy your freedom to work and play in the connected world.

BITDEFENDER INTERNET SECURITY

With the 2011 version of **BitDefender Internet Security**, a lot of attention has been given to creating a personalized user experience. In addition to the proven effectiveness of the software's antivirus, antispam and online security measures, the program is fully functional in its default modes but it's also easily customizable to meet your specific requirements. Just a few minutes after installation, your PC will be protected by one of the best internet security suites around.

BitDefender Internet Security suites offer comprehensive PC protection at an extremely competitive price. For an unbreakable internet security solution to malware of every stripe—from viruses to spyware—BitDefender Internet Security is hard to beat. This year's version includes souped up security features, real-time search results analysis and enhanced support features.

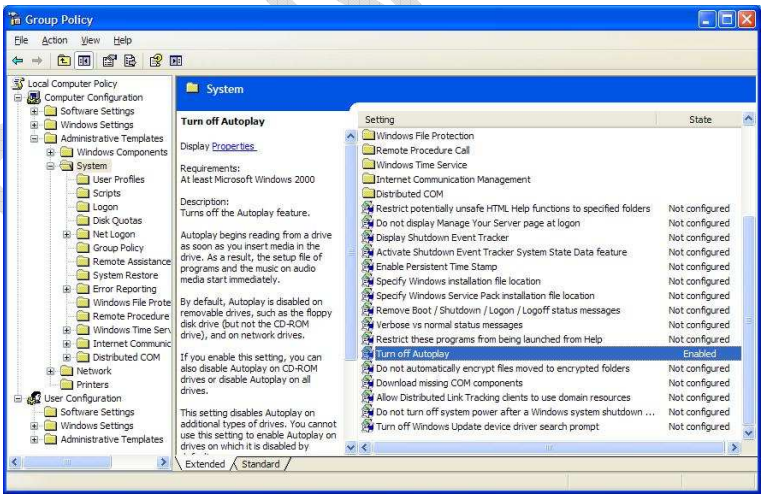
It provides only the basic elements of such a suite, leaving out features common in other packages, such as Web browser protection, backup, and parental controls, and it costs more than any other suite we tested. One extra utility, called SysInspector, is included, but it's geared more for the high-end user, and alone is not worth the extra cost. Eset's traditional malware detection capabilies are adequate.

Eset's user interface is bland, employing a cool-blue-and-white color scheme with a navigation pane along the left side of the window. It has two modes: standard (simplified configuration choices) and advanced (more configuration choices). Various graphs chart network and system activity in both the standard and advanced interfaces.

PRECAUTIONS TO TAKE

It’s always on you that how you keep your system away from viruses. There is always a chance that even after taking all those precautions above you may get infected. Here we are going to explain you some precautions that you should keep in mind while using your pc. I should tell you, the most important of all these precautions is to update your antivirus software regularly as it is the most basic protection of your pc from viruses.

- **Turn off the auto run feature**: Using this feature operating system helps you to find the appropriate application for files in a cd or pen drive while you insert that new device to the system. After searching the system os will give you a list of applications with which you can handle the files in a cd or flash drive. Viruses can take advantage of this system by putting themselves to the pen drive and placing autorun.inf file in that drive for executing the malicious code.

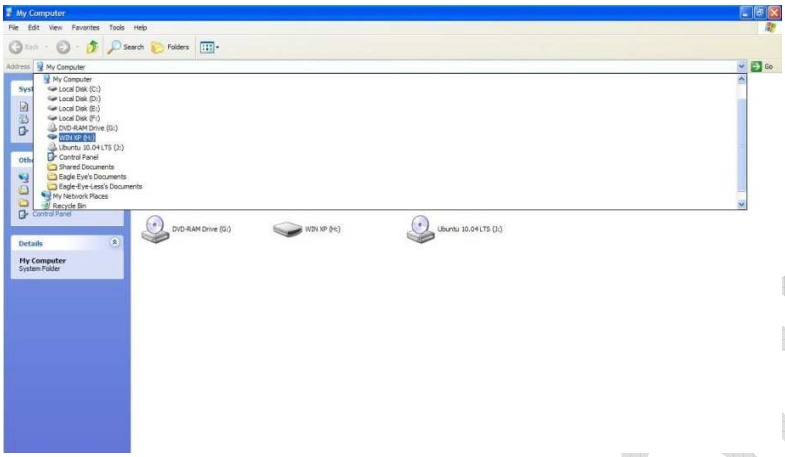


To disable the auto run feature follow the steps given below:

- Go to start menu and type gpedit.msc in the run command.
- From the window opened expand the section named system folder in the Computer Configuration>Administrative Templates section.

- Find the option Turn off Autoplay and double click it to open the properties window.
- Select the Enabled option and apply your selection to disable autoplay.

- **Open pen drive or any other autorun enabled device without double clicking the device from my computer :** Double clicking and opening such devices may put your system into trouble as a hidden malware can be run while you do this double clicking. So the best precaution you can take is not double click but opening the device in some other different way rather than the traditional double clicking. We will explain some of the best possibility other than the traditional way to open your device and view the files.



  - Open My Computer
  - Select the removable device from the dropdown menu at the top like in the picture.

- **Delete first, ask questions later:** When in doubt about the origin of an e-mail, the best thing to do is delete it without previewing or opening it. However, some viruses, such as Klez, propagate by fishing in people's address books and sending themselves from any contact they find to another random contact. You can spread a virus just by having people in your address book, even if you don't actually e-mail them anything. They'll receive it from someone else in your address book, which really makes life confusing.

- **Beware of virus hoaxes:** E-mails warning you about viruses are almost always hoaxes. You may be tempted to believe them because you typically receive them from well-meaning friends, who received them from friends, etc. These e-mails themselves usually aren't viruses, but some have actually fallen into the hands of hackers who loaded them with viruses and forwarded them merrily on their way as a sick joke.

- **Beware of filename extension:** The extension of a filename is the three characters that come after the dot. Windows now defaults to hiding filename extensions, but it isn't a good idea. Just being able to see a suspicious extension and deleting the file before opening it can save you from a virus infection. To see filename extensions in all your directory listings, on the Windows XP desktop, click Start button | Control Panels | Folder Options | View Tab. Clear the check box for Hide extensions of known file types. Click Apply | OK. System files will still be hidden, but you'll be able to see extensions for all the files you need to be concerned with. Viruses often live on files with these extensions – .vbs, .shs, .pif, .Ink – and they are almost never legitimately used for attachments.

- **Disable the .shs extension:** One dangerous extension you can easily disable is .shs. Windows won't recognize it and will alert you before attempting to open a .shs file. The extension is usually just used for "scrap object" files created in Word and Excel when you highlight text and drag it to the desktop for pasting into other documents. If this isn't something you ever do, or you have Word and Excel 2000 or later, which allow you to have 12 items on the Clipboard, click the Start button | Control Panel | Folder Options | File Types tab. Under Registered file types, scroll down and highlight the SHS extension. Click Delete | Yes | Apply | OK.

- **Beware of double extensions:** When you turn on your extensions in Windows, you'll be able to detect viruses that piggy-back themselves onto innocent looking files with a double extension, such as happybirthday.doc.exe. NEVER trust a file with a double extension – it goes against Nature.

- **Beware of unknown .exe file:** A virus is a program that must be executed to do its dirty work, so it may have an .exe extension. Unfortunately, this is the same extension used by legitimate program files. So, don't panic if you find files named Word.exe or Excel.exe on your system – they're your Microsoft software. Just don't EVER open any file with an .exe extension if you don't know what the file's purpose is.

- **Watch out for icons:** Viruses in attachment files have been known to assume the shape of familiar looking icons of text or picture files, like the wolf in the hen house. If you receive an unexpected attachment, don't open it without first running it through your anti-virus software.

- **Backup critical data on a regular basis:** I now this seems obvious and everybody should backup up their important data as a matter of course, but think for a moment, when was the last time you backed up all of your essential data? It can be a pain to do depending how much you use your computer and how much data you need to back up, but if you suffer an attack from a serious virus, you will be very glad you took the time to ensure the safety of your data.

RULES TO FOLLOW WHILE INSTALLING YOUR FAVOURITE SOFTWARES

Softwares are the ones those put life to your system. Without installing a single extra software you might not be abe to run your system up to your purposes. Though one cannot be 100 per cent safe, there are some simple rules one can follow while installing any software for that matter, to ensure that spyware applications do not install themselves on your computer.

- Download software only from trusted and reliable sources. If at any point you are unsure about the the trust-worthiness of a download source, it would be advisable to look elsewhere. If you are a person looking for cracked softwares, there is always a chance that you might get in to trouble as 90% of them comes with a virus of spyware. So its always wise to choose a freeware or genuine software rather than bringing youself trouble. Some of the mose popular sites for downloading freewares are:
    - www.softpedia.com
    - www.cnet.com
    - www.filehippo.com
- Be sure that you have read and understood the licence agreement of any software you are installing. Look for sentences like "When you agree to these terms you agree to allow third-party software to be installed on your computer." Immediately avoid such programs.
- If you really want to install a software you downloaded, but are not sure of its integrity, you should ask someone who knows more about the subject. Even a simple Google search should bring up some answers.

SOME OTHER MAJOR INTERNET THREATS

Only viruses are not your enemy, getting rid of viruses is always good but you should always be aware of the other threats existing there in the wild. I am going to explaing some of the popular threats out of them to keep you safe while you are online.

PHARMING : Like phishing is the art of creating a fraud website like one poular one existing already, pharming is another attempt by hackers to divulge personal information from you, and eventually, your money. Pharming is basically the process of redirecting your browser from the site you originally wanted to visit to a malicious one. But the way you get caught in the pharmers' scams is because the sites are designed to look like the ones you originally wanted to visit. In this way they deceive you, bring you to their sites, and make you give away information.

Its very difficult to find out and block pharming but there are some precautions you can take to prevent this from happening.

- As always, keep your anti-virus and anti-spyware scanners up-to-date.
- Check whether the URL is an HTTPS rather than a HTTP.
- The last and the best thing one could do is to be alert.

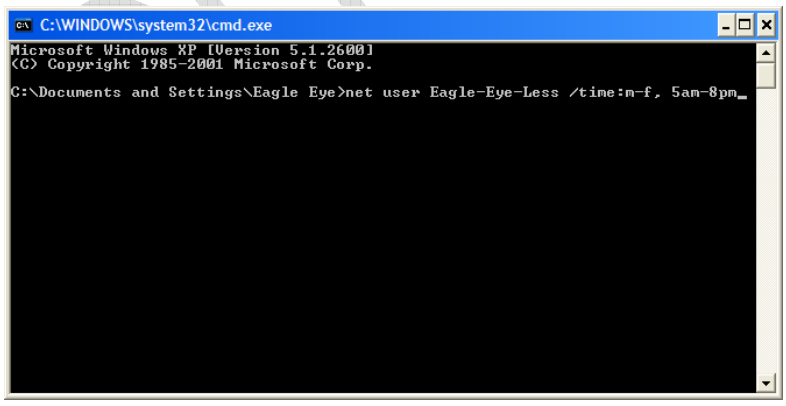
E-MAIL SPOOFING

E-mail spoofing implies changing your name in an e-mail so it looks like the e-mail came from someone else, or some-where else. Spammers and phishers use this technique to hide the origins of their e-mails. Basically, the spammers change the "From", "Return Path" and "Reply To" fields of the mails they send, and make their mails seem like they have come from somewhere else and that they've been sent by someone else. Again, the purpose here is to get unsuspecting users to divulge personal information.

There are some reasonably simple ways one can tell whether an e-mail is a spoof or has been sent from a genuine e-mail address.

- Always check the from address of the e-mail. with spammers using randomly generated e-mail addresses, it is likely that the "From" address will be a jumble of words.
- Check SSL certificate of the mail to ensure that it is from the source it is supposed to be from.
- Check for disguised URLs in the body of the e-mail. If the URLs are long and have several characters in them (for example, www.hotmail.com-SECURITYCHECKrt6uw9ru>shwideoifj123>AccountMaintenance-dnif82jr-4md>gobargas.co.in) then the links are probably fake.
- Apart from this, do the same checks that you would do to check whether the e-mail was from a phisher or a spammer.

A PARENTAL GUIDE TO PROTECT YOUR CHILD



Preventing the user from logging on to the system

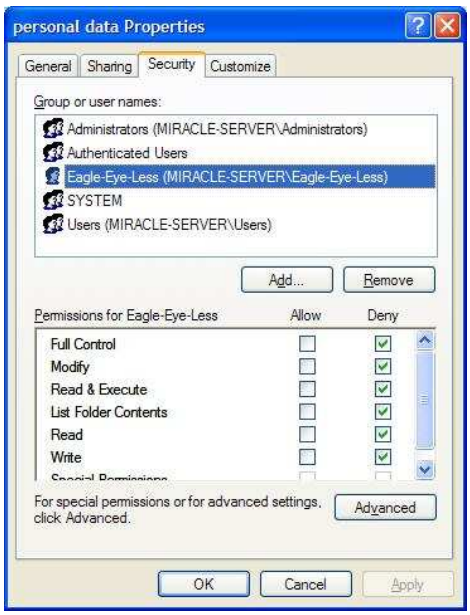
In Windows XP, you can prevent your child from logging on the system in apecified time limit rather than logging on every time he/she wants. Suppose you have a user named ***Wow*** and you want this user to be allowed login only between 5.00 PM and 8.00 PM, on Monday to Friday. To make this happen follow the steps as explained:

- Open command prompt using Run or from the path "C:\WINDOWS\system32\cmd.exe".
- At the command prompt type in the following:

- net user <User Name> /time:m-f,5pm-8pm
- This command will prevent the user from logging in any time other than 5.00 PM to 8.00 PM.

- You can change the days using the switches m, t, w, th, f, s, su.

User access restriction policies



You might have very important information stored over your system, like files containing personal data and financial documents. You can easily prevent other users from accessing such files or folders using Windows XP Professional's builtin user access restriction policies. Suppose you have a folder named "personal data" and you want this not to be accessed by any person who uses your system, I will tell you how.

You need to deactivate simple file sharing as I have explained above to use this protection. If you have already done that lets move to the next step.

- Right click the folder and select properties.
- Select the security tab in properties and click the Add button.
- Now find the user you want to deny the access from the windows opened by clicking Advanced and then Find Now buttons.
- Select the user name from the list and press OK.
- Now tick all the options listed in the deny coloumn of the window and apply all the settings.
- Now the user wont be able to access of delete any of the files from that folder without any other third party software installed.

Parental Control Software

Parental control software makes it harder to find inappropriate material on the Internet or to do things that "parents" don't want. The criteria I've used include these four main components of parental control plus compatibility with browsers and operating systems:

Block addresses – to avoid specific Internet addresses (URLs or IP addresses)

Filter content – to identify inappropriate material

Manage usage – to limit Internet access by setting time limits and time quotas

K9 Web Protection is a free parental-control utility from Blue Coat Systems. If it suits your needs, the price is certainly right. However, it lacks quite a few features I've come to expect in parental control software.

K9 breaks down Web sites into 24 commonly blocked categories and 44 other categories, plus uncategorized sites and Web ads. The commonly blocked categories include the expected—porn, gambling, nudity, hacking, and so on. The other categories, things like humor, games, and shopping, are probably more useful in the company's business-oriented filtering product. Taking both sets together, that's 66 distinct categories—more than any parental product I've reviewed lately.

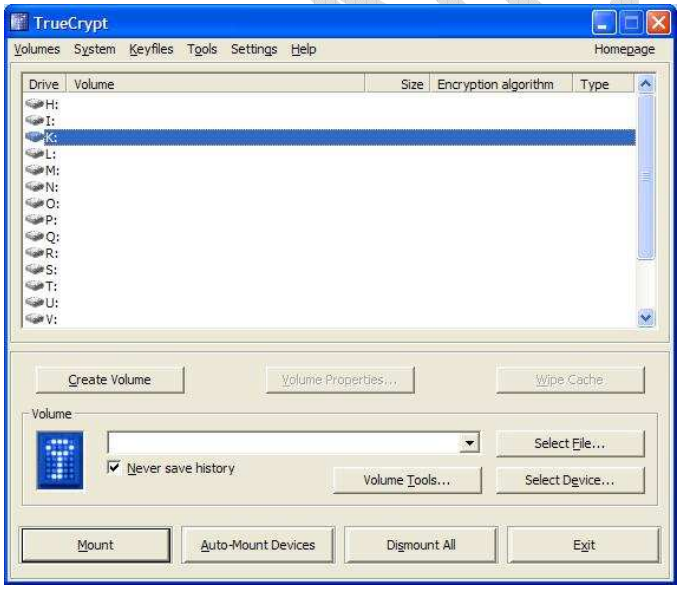
If you prefer, you can set the product to monitor all Web surfing without blocking any categories. The log will still list and categorize all sites visited. Note, though, that although the date and time of each site visit is logged, the user account that visited the site is not.

Like Webroot and Norton, K9 can force kid-friendly "safe search" mode for several popular search engines. It specifically manages Ask, Google, MSN, Yahoo, and others. And you can set it to block use of any non-childproofed search engines.

PROS: Small, fast install. Cloud-based filter blocks objectionable Web-site categories. Full weekly schedule for Internet access. Browser-independent and tamper-resistant. Filters HTTPS sites. Logs and categorizes all Web sites visited.

CONS: No per-user configuration. Hard-to-read log omits username. Weak phishing protection. No IM control or monitoring. No e-mail notification. No remote management.

DATA SECURITY AND HOW TO



Data security is a sensitive topic. The increasing number of operating system features and Web services introduces more options for accessing, modifying—and losing—data. Yet, many people don't really have a true security plan in place for protecting their data.

What would you think if an unauthorized person gained access to your personal files? Would someone be able to find information that is meant for your eyes only? Would they be able to do harm? I'd guess that they probably could—at least, that's the case with *my* personal files. Whether data is personal or business related, important files have to be secured, and that brings us to a potentially incredible solution: TrueCrypt.

TrueCrypt has been around as an OpenSource encryption tool for a few years. Its main application was the creation of so-called *encrypted containers* to store files in a secure manner. Containers can even be mounted as Windows drives in recent versions of the tool. With the introduction of TrueCrypt 6.0, the

tool was given the ability to encrypt an existing Windows installation on the fly, which means adding the extra layer of security by encrypting the entire system drive or partition. In our tests, this worked really well.

The product matches the features offered by Microsoft's BitLocker and offers a couple of interesting additional features, such as the ability to create a virtual encrypted volume that is mounted as a drive letter or associated with a virtual folder. In other words, you can store all of your critical data files on a separate, encrypted disk volume and then access those data files by associating a drive letter with the volume and entering the associated passkey.

FIREWALL AND SYSTEM PROTECTION

Firewalls are an important part of internet security. They guard systems and networks from hack attempts and other malicious unauthorized activity. Firewalls can help and protect you from being attacked by malicious hackers and deadly malware roaming around your network and internet.

Firewalls works as shield in between you and the outer world. When a malicious activity is detected they can produce an alert regarding the activity and you can choose any action that you would find to be appropriate for the situation. Although Windows comes with a built-in firewall, it's not that helpful in fighting malware or hackers reaching your system. So it's always important to have a good firewall installed and configured on your system.

We had a talk over antivirues in the above section, all of the above specified paid antivirus solutions have a firewall attached to them but it is more secured to have a dedicated solution for network breach in your system like I said for spyware and adware. I would like to introduce you to one of the most used and efficient freeware firewall out there.
Comodo Personal Firewall

If you're looking for maximum protection from a firewall, and are willing to put up with a number of annoyances, you'd do well to install the free Comodo Firewall, an extremely effective protection tool for keeping yourself safe from Internet dangers. It blocks Trojans, hackers trying to take control of your PC, and other Internet and network threats--and does it without charging you a penny.

For basic operation, that's all that you need to know, although if you want to customize Comodo's functioning, you can do that as well. There's also a wealth of techie information available, but most people won't need it, and will be satisfied to let the firewall work on its own.

More important than interface for a firewall is effectiveness and here Comodo Firewall Pro shines, according to the Matousec.com set of firewall tests. It rates Comodo Firewall Pro well ahead of other firewalls--over the last year, the firewall rated 95% every time it was tested. By way of contrast, Norton

Internet Security's firewall ratings range between 66% and 71%, McAfee's were at 12%, Panda Internet Security between 4% and 12%, ZoneAlarm Free at 11%, and ZoneAlarm Pro at 72%.

Should you use this firewall? If you're willing to put up with a very annoying installation procedure, and don't mind occasional interruptions, Comodo Firewall's a keeper. It's a strong firewall, and you certainly can't beat the price. If the installation issues turn you off, you might want to try a less intrusive firewall such as ZoneAlarm, or merely use the ones built into Windows.

SOME TIPS TO AVOID IDENTITY THEFT WHILE YOU ARE SHOPPING ONLINE

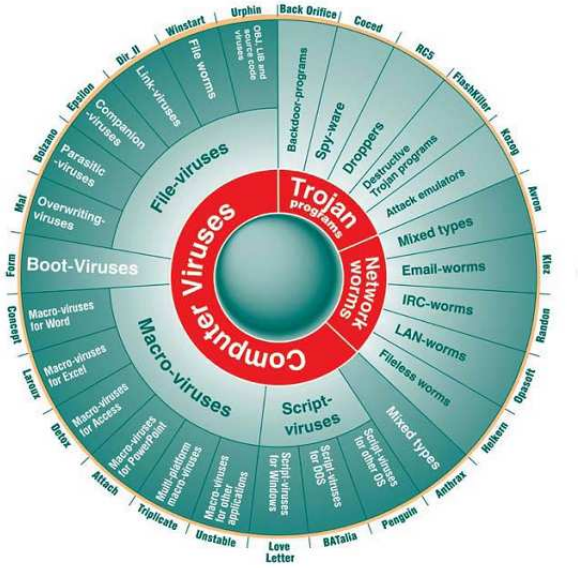
All it takes is one wrong click of the mouse for a criminal to follow every move someone makes online - every password entered, credit card number typed, and conversation that takes place. Fortunately, there are some easy ways to prevent falling victim to an online scam. Following are the major precautions you can take while you shop online. Although it’s inevitable to completely protect you from being hacked, let’s remember what our grand fathers have taught us “Precaution is better than cure”. So, here are your precautions:

Check for a secure internet connection - Wi-Fi hotspots at coffee shops, hotels and restaurants provide easy online access to internet users. However, it's important to make sure the connection is secure. The same goes for home internet connections. Jumping on an unsecure network may be simple but it's not safe. Hackers can easily access internet activity when the network isn't protected.

Purchase with caution - Credit cards offer better protection than debit cards when shopping online. Before making an online purchase, verify the site's credibility by checking for the https:// prefix in the web address. The 's' following http stands for 'secure' so consumers can shop online and know their personal information is safe.

Avoid clicking e-mail links - Never access a bank account, make a purchase or send personal information directly through a link in an e-mail. Even if it looks legitimate, it could give criminals the ability to view personal information. Type the specific web address into the browser and go from there. Also, be wary of e-mails that ask you to update passwords and other personal information.

Get creative with passwords - Using the same password across every online account is a common, but dangerous mistake. If an internet hacker gets a hold of one password, they can do damage across a variety of personal and social networking sites. Consumer Reports suggests creating unique variations of the same password.



Malware, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. [Source: Wikipedia]

VIRUS: The term virus (vital information resource under size) is used for a program written by a computer programmer which has infected some executable software and which causes that software, when run, to spread the virus to other executable software. Viruses may also contain a payload which performs other actions, often malicious.

WORM: Worm is also a virus but automatically transmits itself over a network to infect other computers. It too may carry a payload. Worm is more powerful and harmful and worm automatically infects system software's.

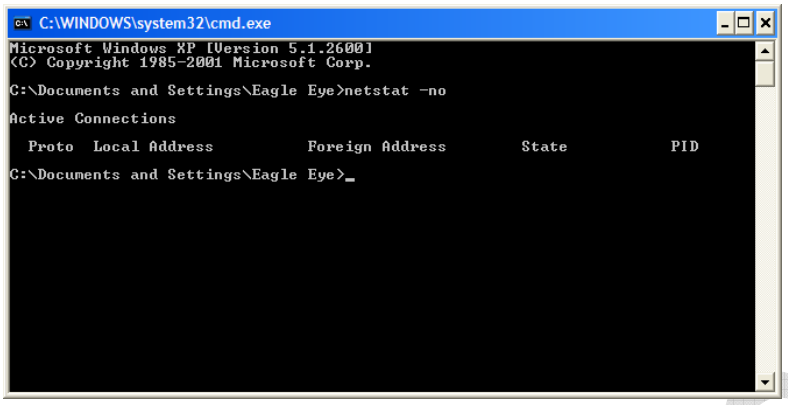
TROJAN HORSE: is also a type of virus which is used to control remote machine without system owner knowledge. Trojan has two parts : 1. server 2. client , Server handles all infected remote computers' connections and client is used to infect victim computer system. Every Trojan has its associated port number for communication over internet or LAN.

ROOT KIT: Root kit is also a very powerful kind of remote access tool. Hackers use this tool to keep their connection with the compromised system alive. But root kits are far more advanced and very destructive compared to a Trojan Horse as they are implemented on the operating system kernel level. So, it becomes very difficult to detect and remove these kinds of threats. There are some specialized tools provided by antivirus companies for root kit detection and removal as your antivirus does not detect or remove them. Most of the antivirus companies have their own root kit removal tools and there are also some stand alone tools such as ***root kit hunter.***

SPYWARE: Spyware is a piece of software used basically for compromising information about a user, their computer, browsing habits. In most cases such piece of software's are found when we download cracked software's from any unknown website. Spywares hide inside and behave like legitimate software to the user and they send all the information collected to the other end person whenever they get a chance. Some of them can do vast destructions such as downloading other malware, remote control of your system and other devices etc.

CHECKING FOR UNWANTED OPEN PORTS

It is always a good habit to check your incoming and outgoing connections while administaring your system. Windows provides some commands to do this check yourself. If you find any unknown connections it is best to terminate those connections immediately. Use netstat command in dos prompt to find out unwanted open ports:



This command will provide you with a list of existing connections of your computer to the outer world. Here the coloumn called PID (Process ID) is very important as it denotes the ID of the process that is behind the connection. Check for the process using the task manager or one of my favourite process viewing application Process Explorer to find the correponding process and make sure that the process is not a harmful one. If you find the process suspicious, your first preference will be to terminate the process.

To terminate process use; ***c:\> taskkill /PID <PID>***

Process Explorer, FPort and Tcp View are some of those tools you will find handy while checking your system for unknown virus hoaxses.

SOME WINDOWS FUN TWEAKS

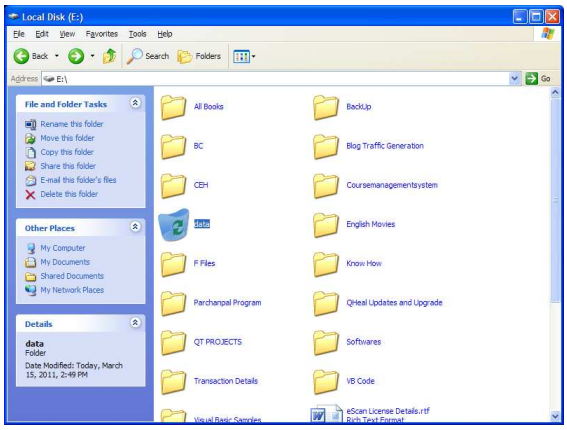
Before we go so deep you should be aware what is registry in Windows. The registry is a simple, hierarchical database of information that Windows operating systems (and some applications) use to define the configuration of the system. Originally, in the early, simple days of Windows (16-bit Windows versions especially), the same information that is now stored in the registry was stored in text files.

- **How to hide file and folder super hidden:** It is a 100% safe and free method to hide a file or folder from others in your system without using any application.For this ,open dos prompt and type:

  To hide - C:\> attrib +a +r +s +h foldername /s /d
  To show - C:\> attrib -a -r -s -h foldername /s /d

  The main limitation with this method is that, if hide protected operating system files option is uncheck in folder options, victim can see ur files so disable folder options feature.

- **Change any folder to recycle bin:** For changing your target folder to Recycle Bin type the following lines to the Notepad and save the file as *Desktop.ini* and save that file to the folder that you want to change to



Folder changed to Recycle Bin

recycle bin. This method is very helpful in hiding your important folders for data security.

[.ShellClassInfo]

CLSID={645FF040-5081-101B-9F08-00AA002F954E}

We save desktop.ini in e:\data folder and then we open dos prompt and type the following command, which will convert the data2 folder into recycle bin.

e:\> attrib +a +r +s data2 /s /d

To change the folder back to the original use the same command with (-) signs infront of the letters a,r and s. To change any folder into control panel and mycomputer use following *CLSID: Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}*

- **Disable Log Off and Run feature in Windows:** Type down the following lines to the Notepad and save the file as *logoff.reg* , after that run the file to disable the Log Off feature of your Windows operating system.

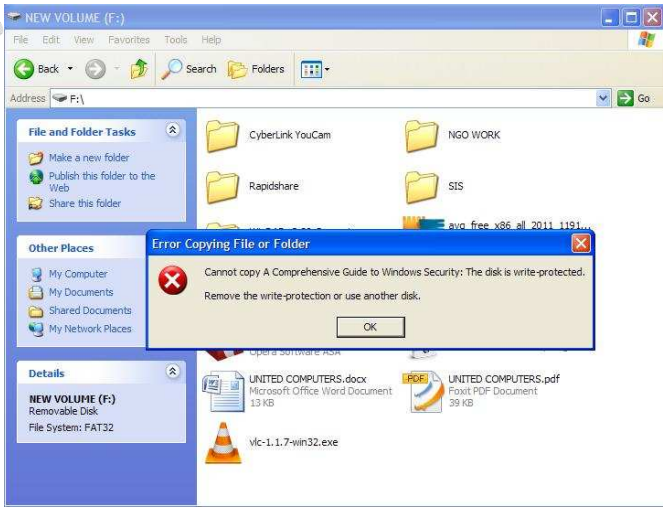
  Windows Registry Editor Version 5.00
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
  "NoLogoff"=dword:00000001

  To disable the Run feature follow the same steps other than saving the file with the name *run.reg.* Use the following lines to disable the run feature.

  Windows Registry Editor Version 5.00
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
  "NoRun"=dword:00000001

  To bring these features back just change the number in the above line to *00000000.*

- **Disable writing to USB Drives:** A major concern at organizations is allowing users to plug in a USB Flash Drive, because they could so easily copy corporate data. Since Windows XP SP2, you can disable writing to USB devices altogether using a simple registry hack. Paste the following code into a notepad file, and then save it as a registry file (file.reg). Double click it and now you have successfully prevented the write access to the USB drive.



Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000001

If you want to enable the write access again, then copy this code and paste the code into a notepad file, and then save it as a registry file. Double click it and write access will be enabled again.

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000000'

CONCLUSION

In my opinion we have dealt with most of the problems and their solutions in the above chapters, so its time to conclude the discussion with all what we have discussed. Typically, the session above is a simple matter of identifying areas where your PC security could use some beefing up and fixing them. Hopefully, this guide will have given you a good idea about what you need to protect your PC. Here is a quick checklist to remind you.

- Install antimalware software
- Install a good firewall
- Install one altiphishing software (the latest Avast comes with one)
- Install one network monitoring system
- Update all your software including your operating system
- Create backup of your important data regularly

I hope this guide will improve your concept about your Windows security. We've touched on a lot of information in this guide. We've talked about malware threats, scams, the anti-malware software you need, freeware alternatives, and more. On the next ediction of this guide I am expecting to inclde more and more information regarding security.