PC Security and Maintenance

by
IMRAN GHANI

- Major sources of danger.

- Important steps to protect your PC.

- PC Security Tools.

- PC Maintenance Tools.

- Tips.

- Running malicious codes on your computer due to system or application vulnerabilities or improper user action.

- Virus, Worms, Trojans.

- Spam or unsolicited e-mails.

- Spyware and Phishing.

- Unauthorized access.

- Faulty system configuration.

- Malfunctioning of PC hardware.

Facts about PC Security Management:

- Computer Security is not an add-on or something external, it is part of everything you do with computer.

- Not "one-size-fits-all", but appropriate for the needs and vulnerabilities of each system.

- In most of cases, it is simple common sense plus a little information and care.

PC Security- Steps to protect your PC

1. Prevent unauthorized access.

2. Implement strong security policies.

3. Block, detect or disable computer Viruses and Worms.

4. Block dangerous e-mail attachments.

5. Block spam or unsolicited e-mails.

6. Update operating system, application, and antivirus regularly.

7. Create and analyze security logs.

1. Windows Logon (Password and User Accounts)

2. Local Security Policy

3. Windows Firewall

4. Security Settings in Internet Explorer

5. Antivirus

6. Anti Spam and E-mail security

7. Windows Updates

8. Event Viewer

Advantages of system based Access Control:

- Multiple levels of user and group privileges.

- Per user based password protected "My Document" folder.

- Customized look of Windows and Desktop.

- Per user based list of Web Favorites and recently visited website.

PC Security- Windows Logon

Use "Local Users and Groups" to manages users and groups of users of your computer. You may create new users and groups, add users to groups, remove users from groups, disable users and group accounts, and reset password.
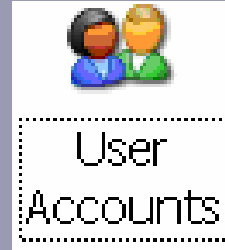
To open "Local Users and Groups":

1. Click Start, and then click Control Panel.
2. Double click Administrative Tools, and then click Computer Management.
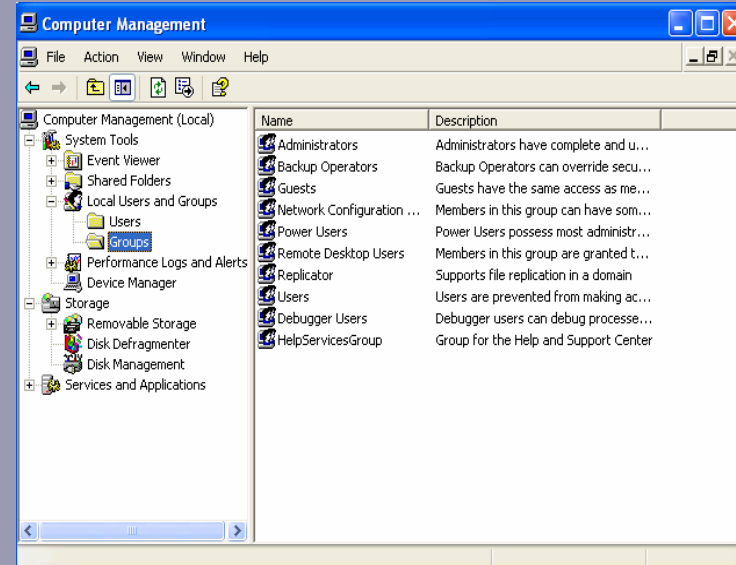
© Imran Ghani, 2006, ighani@ducc.du.ac.in

You may also use "User Accounts" icon in Control Panel to create and manage users.
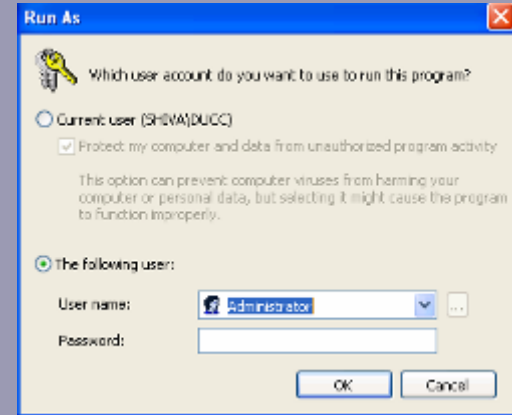

User Accounts

Tip: Always logon and work on your PC with a user account having least privileges. Except at the time of running any required program or re-configuring your system

PC Security- Windows Logon

To start program as an Administrator:

1. In Windows Explorer, click the program executable file that you want to open.

2. Press SHIFT and hold, right click the program icon, and then click "Run As".

3. To log on as Administrator account, click "The following user".

4. In "User name" and "Password", type the Administrator account and password that you want to use.

You may use Local Security Policy to directly modify the following:

1. Account Policy
   - Password Policy
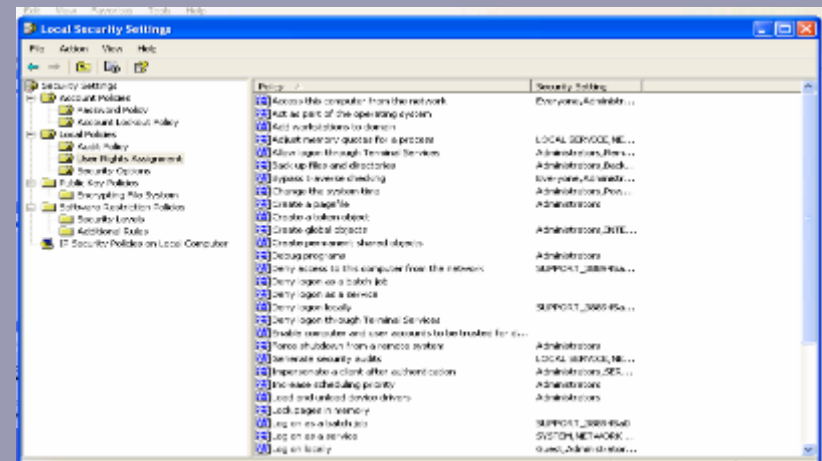   - Account Lockout Policy
2. Local Policy
   – Audit Policy
   – User Right Assignment
   – Security Policy
3. Public key Policy
4. Software Restriction Policy
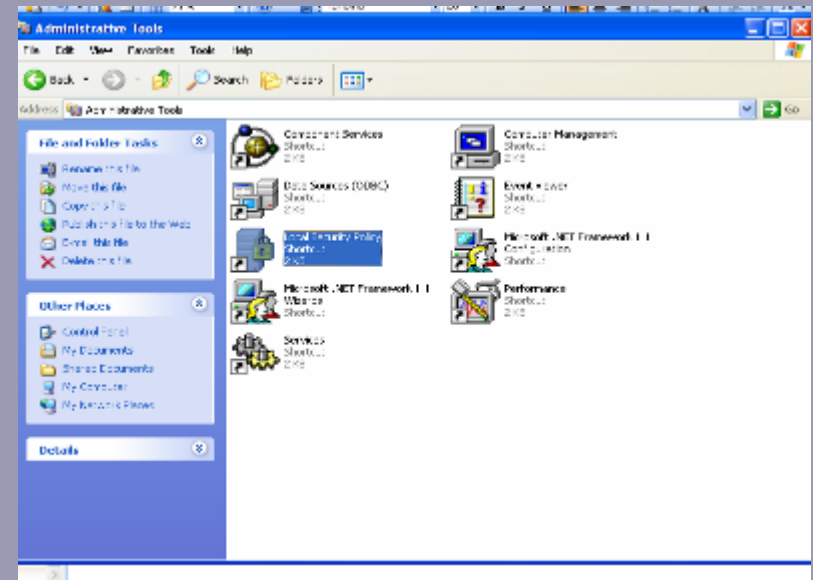5. IP Security Policies on Local Computer

PC Security- Local Security Policy

To open Local Security

Policy:

1. Go to "Start", and click "Control Panel"

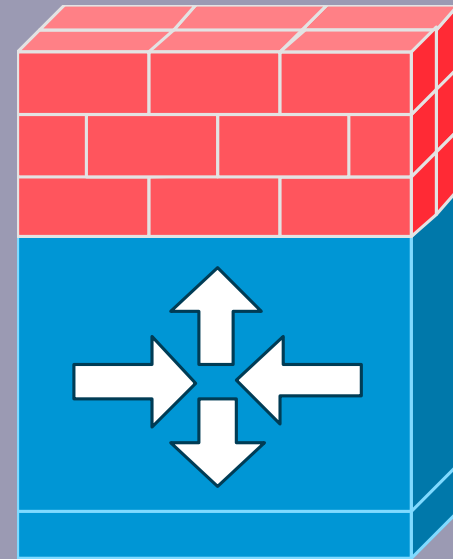2. In Control Panel double click "Administrative Tools"

Firewall:

A combination of hardware and software that, provides a security system, usually to prevent unauthorized access from other network devices.
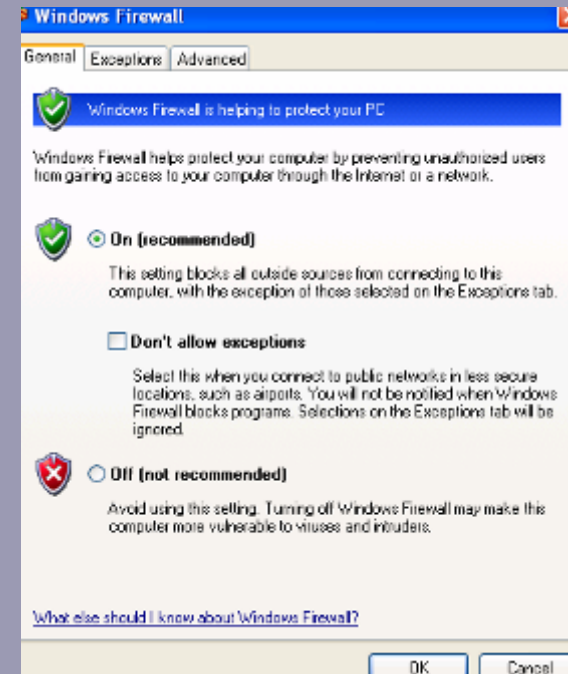
1. Firewall with OS
2. Third party firewall

By default Windows Firewall (in Windows XP with SP-2) blocks unsolicited request to connect to your computer. You can make an exception for programs which you think are required for you. Each time you allow an exception for program to communicate from Firewall, your computer made more vulnerable. Unknown Intruders often use software that scans the Internet looking for computers with unprotected connections. If you have many exceptions and open ports, your computer can become a victim of these Intruders.

To decrease your security risk:

- Only open an exception when you really need it.

- Never allow an exception for a program that you don't recognize.

- Remove an exception when you no longer need it.

PC Security-Windows Firewall

To add a program to an exception list:

1. Log on as an administrator.

2. Open Windows Firewall in Control Panel.

3. On Exception tab, under Program and Services, select the check box for the program or service that you want to allow, and then click OK.
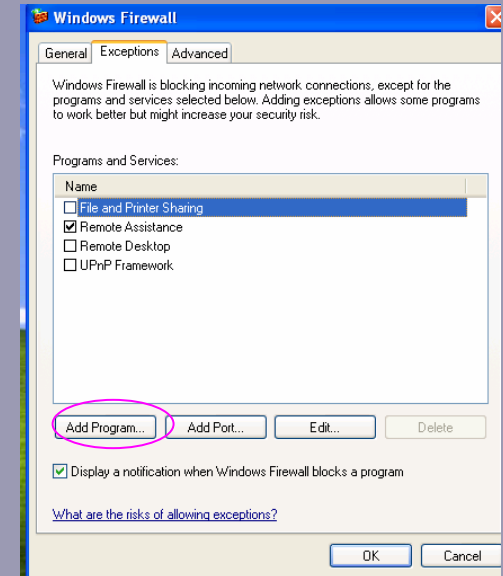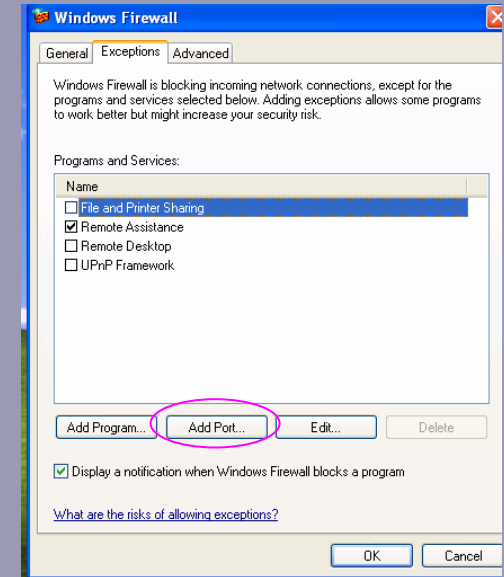
If the program (or service) that you want
to allow is not listed, use "Add a Program"
dialog box.

You may also open ports using "Add Port".

(Adding an exception is preferable to opening a port, because the firewall is only open while the program is waiting to receive the connection).

ftp://download.du.ac.in/mswin/avupdatePack/

PC Security- Antivirus

What is a Virus:

A virus is a program that can be hidden inside another file — it replicates itself and spreads to other files and computers.

Source of Virus:

- Shared files, networks, floppy disks

- E-mail attachments

- Web-based e-mail

- Downloads

- Malicious Web sites

PC Security- Antivirus

What can virus do?

1. A virus (worm) can copy itself multiple times and infect your computer by occupying hard disk space, choking your network bandwidth etc.

2. Some viruses contain code that inflicts extra damage by deleting files or lowering your security settings, inviting further attacks.

3. A virus even format hard disk of your computer.

4. A type of virus (called Trojan Horses) can scan your hard disk and send important information to the source.

5. An e-mail virus can scan your address book and send e-mails using your e-mail account.

PC Security- Antivirus

Attachments in e-mail messages are one of the most common ways that your computer can "catch" a virus. Sometimes just opening the message can trigger the virus.

Be especially suspicious if:

1. The message is from someone you don't know or aren't expecting to hear from.

2. The subject line is strange.
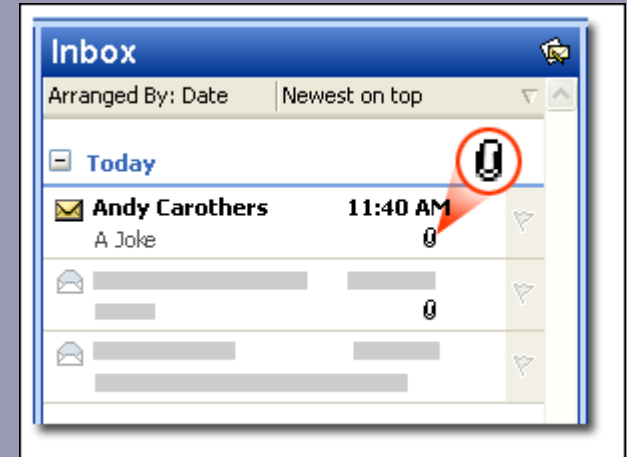
The paper clip icon indicates a message attachment.

Your most important defense against viruses is **antivirus software**:
Install it, use it, and keep it up to date.
This software is essential as a defense against viruses.
Setting up your e-mail and Internet browsing software so that it is more difficult for files containing viruses to make their way onto your computer at all is another good step.

PC Security- Antivirus

Antivirus software is designed to detect *known* viruses. Because new viruses are always being written, it's essential to keep your antivirus software up to date. When a new virus hits the world, the antivirus software manufacturers normally have an update available for download on their Web sites within hours. In addition to using up-to date antivirus software, you should also make sure that it has a "real-time scanning" feature. Real-time scanning checks files before they are opened or used. You may also configure schedule for periodic scanning and automatic up gradation of signature file.
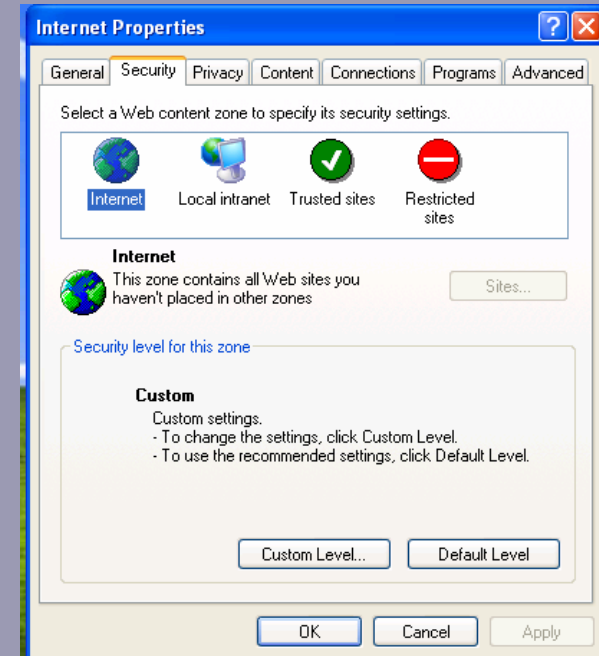
ftp://download.du.ac.in/mswin/avupdatePack/
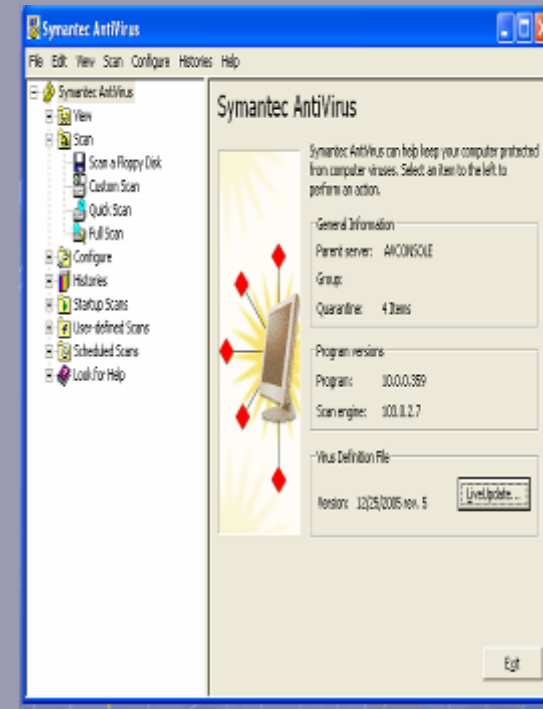
PC Security- Internet Explorer Security

Internet Explorer (IE) provides a number of features that help to protect your privacy and make your computer and your personally identifiable information more secure.

Privacy settings:

1. Specify how your computer deals with cookies. Cookies are files created by a Web site that store information on your computer, such as your preferences when visiting that site. Cookies may also store personally identifiable information, such as your name or e-mail address.

2. Privacy alerts that let you know when you try to gain access to a site that doesn't meet the criteria in your privacy settings.

© Imran Ghani, 2006, ighani@ducc.du.ac.in

Security features:

1. Help to prevent people from gaining access to information that you have not given them permission to access, such as credit card information you enter when shopping on the Internet.

2. Security features can also protect your computer from unsafe software.

3. Block most pop-up windows.

4. Update, disable, or re-enable Web browser add-ons.

5. Enhanced security features to warn you when a Web site is trying to download files or software to your computer.

Configuring Security features of IE:

1. Open Internet Explorer and click "Tools".

2. Click "Internet Options", and go to "Security" tab. Here you may define security for Internet and Local Intranet. You may also list the names of "Trusted" and "Restricted" sites.

3. You can use "Custom Level" button to set the level of security according to your need.
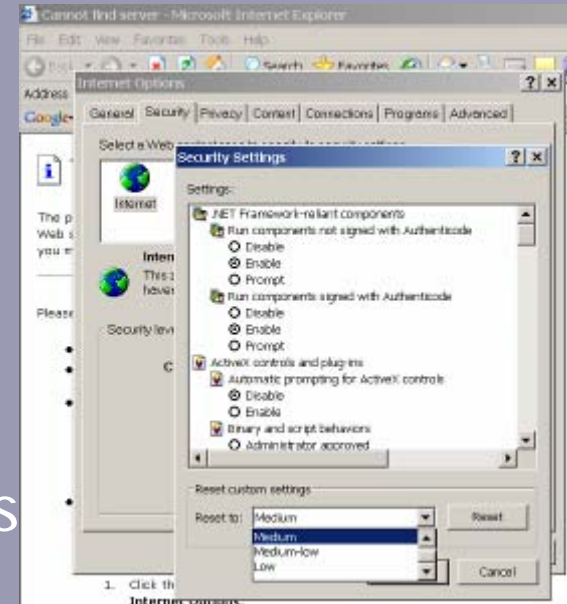
PC Security- Anti Spam

Junk e-mail (Spam) is a significant problem for computer system users. We must spend time dealing with spam in our electronic mail boxes because we rely on e-mail as a communication tool both at work and at home.

Junk E-mail Filter

Junk E-mail folder   Inbox

PC Security- Anti Spam

Tips to help reduce in the amount of junk e-mail (spam) arriving in your mailbox:

1. Never respond to unsolicited e-mail. While some unsolicited e-mail messages promise to take your name off their mailing list, they are usually confirming that they have a live address by asking for a response.

2. Use an alternate e-mail address in public forums, such as newsgroups.

(Cont.....)

© Imran Ghani, 2006, ighani@ducc.du.ac.in

3. Do not give out your e-mail address unless you know how it will be used. If a web site asks for your e-mail address, be sure you know what it intends to do with that information. If you cannot find a privacy statement on a web site asking for your e-mail address, do not provide your email address.

4. Use a filter on your mailbox. Filtering software can help keep unsolicited e-mail a manageable level.

5. Block unwanted sender.

6. Keep your antivirus up-to-date.

7. Keep your Windows up-to-date.

Junk E-mail folder (in MS Outlook):

You may configure Junk E-mail folder in Outlook to deal with spam. If the filter deems a message to be junk, the message is moved to the Junk E-mail folder.
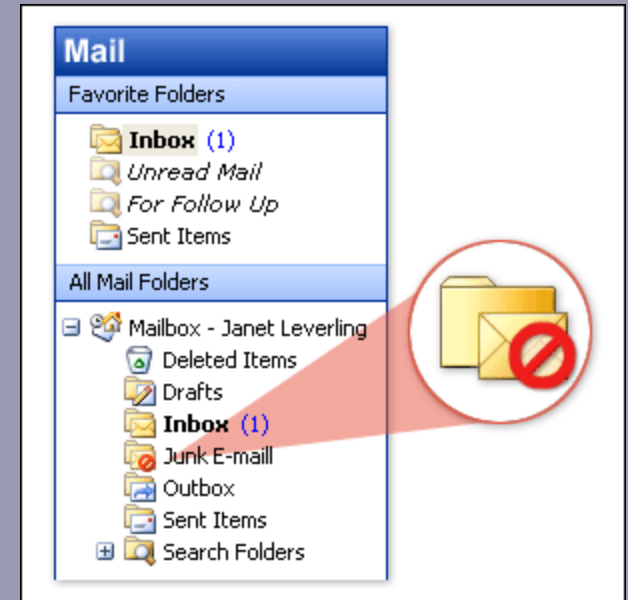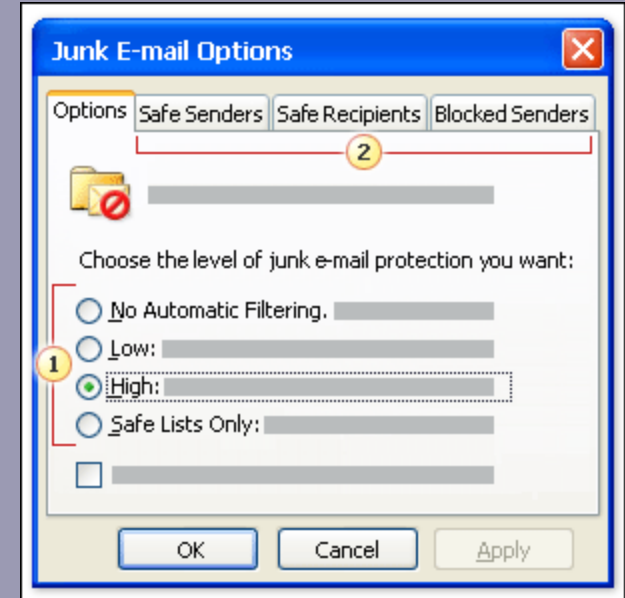

The Junk E-mail folder in the Navigation Pane

Controlling the Junk E-mail filter:

1. Use these tabs to view and modify the Safe Senders, Safe Recipients, and Blocked Senders lists.

2. These options adjust the level of protection. Your choice here determines the filtering applied to incoming messages.

The **Junk E-mail Options** dialog box

Safe or Blocked? You decide with lists:

Messages from or to people on your Safe lists are always allowed into your Inbox.

Messages from people on your Blocked Senders List are banished to the Junk E-mail folder.
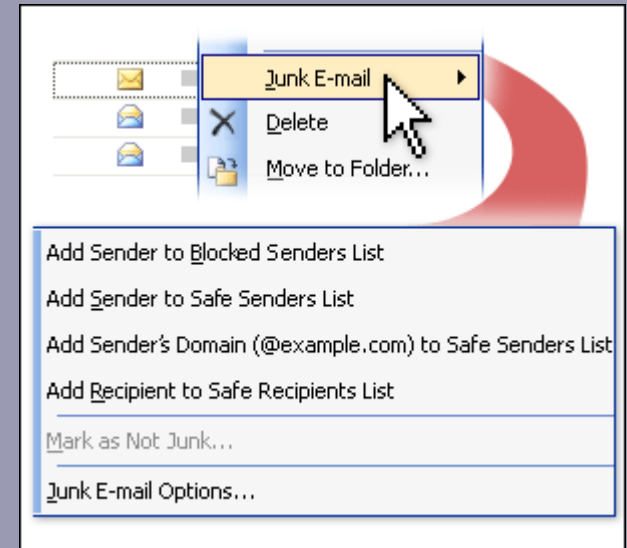
PC Security- Anti Spam

Safe and Block lists:

Your Safe and Blocked lists can evolve as you receive e-mail.

You can add names to these lists directly from messages in your Inbox.

1. Right-click the message.

2. Click **Junk E-mail**.

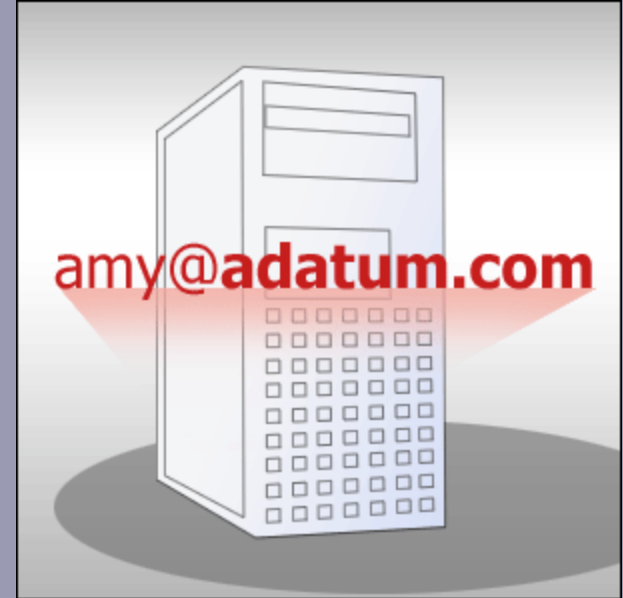3. Choose from the commands on the shortcut menu.

Use a domain name in your Safe or Blocked lists:

A domain name in a Safe list allows all messages with that domain to pass directly to your Inbox.

The domain name is the part of an e-mail address after the @ sign.

PC Security- Windows Update

Windows Update is the online extension of Windows that helps us to keep our computer up-to-date. We may use Windows Update to updates our computer's operating system, software, and hardware drivers. New content is added to the Microsoft site http://windowsupdate.microsoft.com regularly, so anyone can always get the most recent updates and fixes to protect his/ her computer.
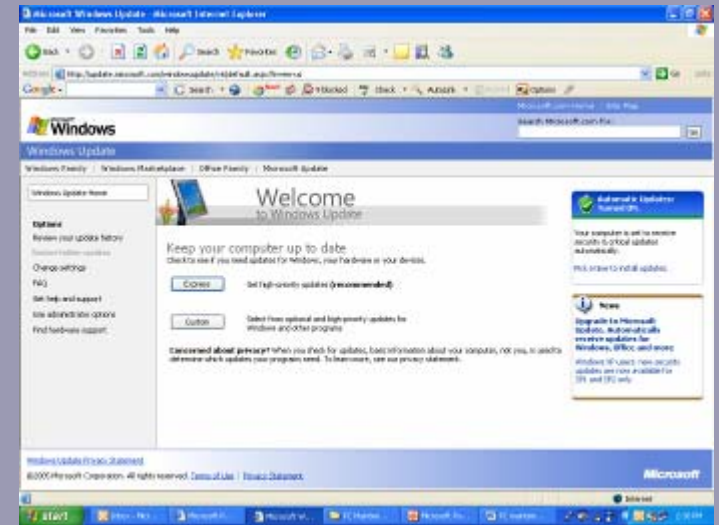
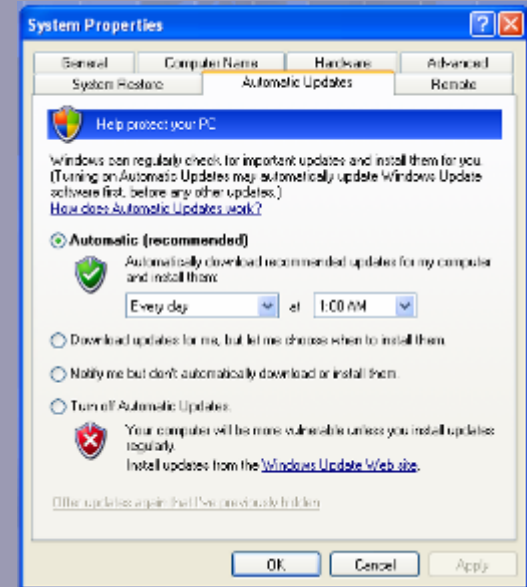Click Windows Update in All Programs list.

Setting your PC for automatic

Updates:
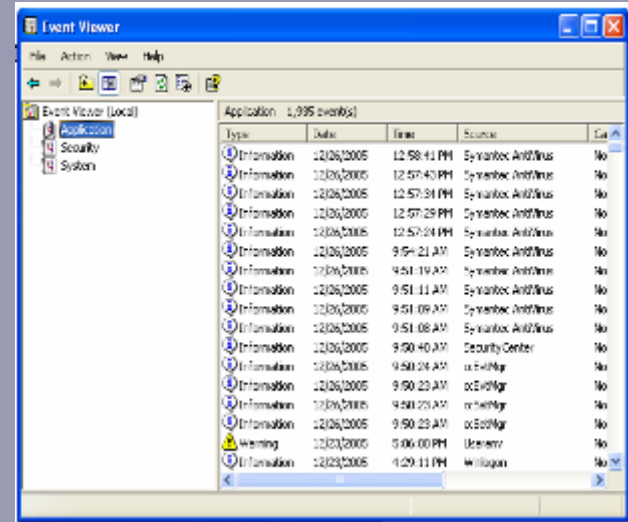
1. Double click System in Control
   Panel.

2. Click Automatic Updates tab and
   select other parameters
   according to your preference.

Event Viewer maintains logs about program, security, and system events on your computer. You can use Event Viewer to view and manage the event logs, gather information about hardware and software problems, and monitor Windows security events.

To open Event Viewer:

- Click **Start**, and then click **Control Panel.**

- Double-click **Administrative Tools**

- Then double-click **Event Viewer**.

© Imran Ghani, 2006, ighani@ducc.du.ac.in

PC Maintenance-Tasks.

Tasks required in order to maintain and improve performance of your PC:

1. Data and System Backup

2. Detecting and Repairing Disk errors.

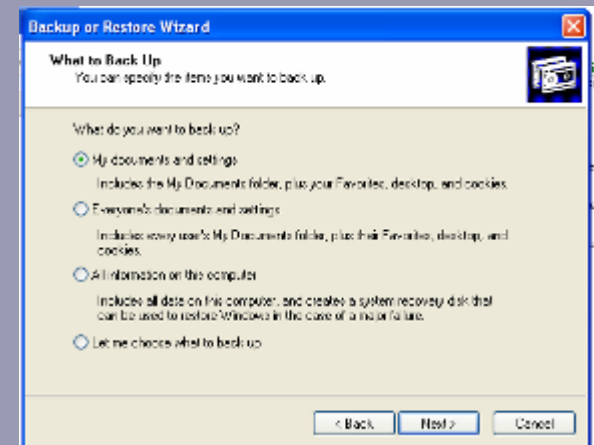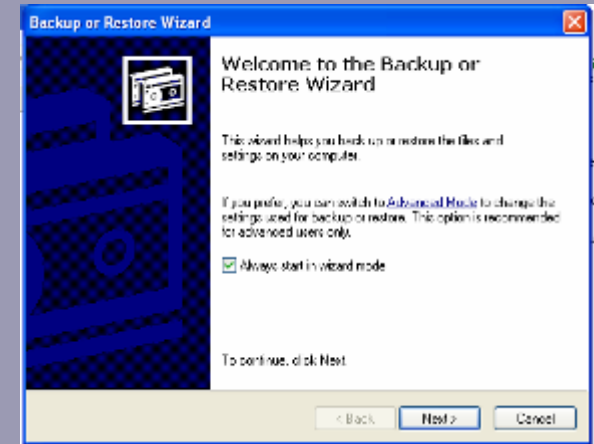3. Disk cleaning.

4. Disk De-fragmentation.

Backup:

You may create System Recovery Disk, which is required to restore the system after major crash. You can also take backup of your data, and favorites, desktop and cookies settings.

To open Backup:

1. Click Start, then click All Programs.
2. Click Accessories, and then click System Tools.
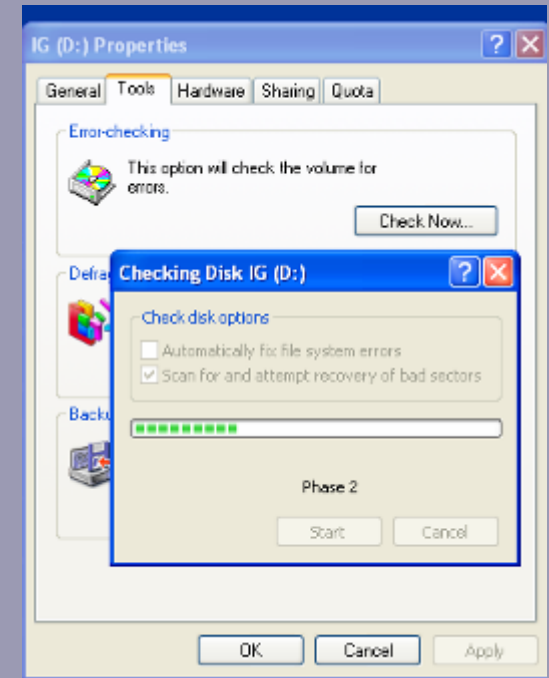3. Double click Backup.

Detecting and Repairing Disk errors:

1. Open "My Computer", and select the local disk you want to check.

2. On "File" menu, click Properties.

3. On the "Tools" , under "Error-checking", click :Check Now".

4. Under "Check disk options", select the "Scan for and attempt recovery of bad sectors" check box.
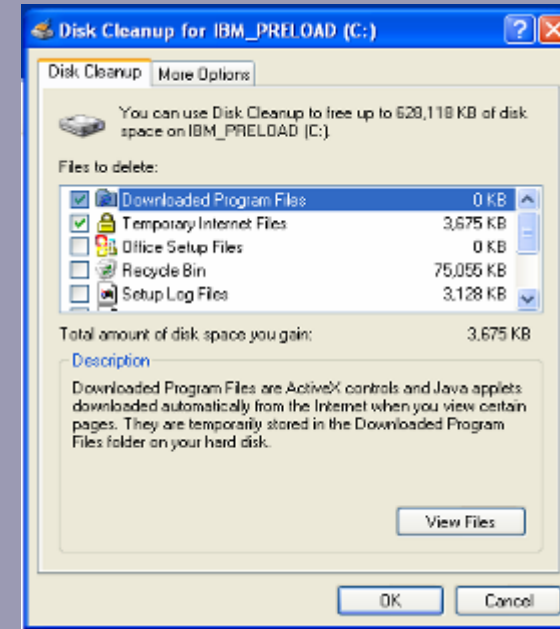
Disk Cleanup:

This tool will detect your PC for temporary files, old setup files, and for not required application software and remove it from your PC.

You may run "Disk Cleanup" tool in "System Tools" of Accessories tab available in All Programs.
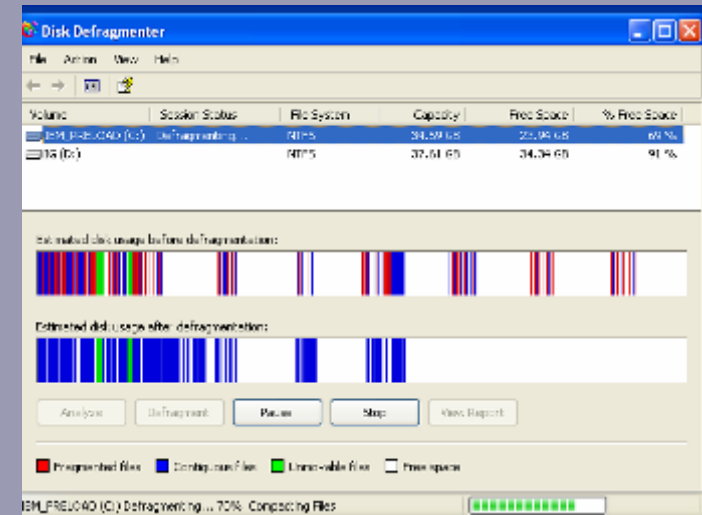
PC Maintenance-Disk-Defragmenter.

The scattering of parts of the same disk file over different areas of the disk occurs over a period of time mainly due to deletion and addition of files on disk. It slows disk access and Degrades the overall performance of disk operations.

You can use Disk Defragmenter tool to analyze local volume (hard disk space), and to locate and Consolidate fragmented files and folders.
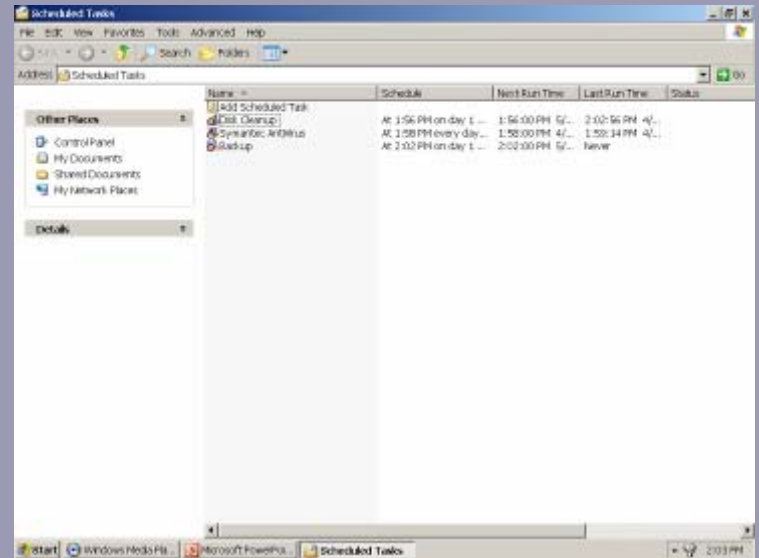

To open Disk Defragmenter

- Click Start, then click All Programs.

- Click Accessories, and then click System Tools.

- Double click Disk Defragmenter.

© Imran Ghani, 2006, ighani@ducc.du.ac.in

You may also use "Scheduled Tasks" program available in "System Tools" to make a schedule for running maintenance tools according to your priorities.

PC Maintenance and Security-Tips

1. Work with your computer with user logon, not with administrator logon for day-to-day work.
2. Keep your computer updated with the latest critical updates and security patches.
3. Keep your Antivirus up-to-date and run regularly.
4. Keep your Office update with the latest critical updates.
5. Keep your Firewall always ON.
6. Back up data regularly.
7. Download files only from trusted sites.
8. Run Disk Cleanup and Disk Defragmenter tools periodically.

Major sources of danger:

Malicious codes, system and application Vulnerabilities, Virus, Worm, Trojan, Spam, Spyware, Unauthorized access, Faulty configuration of system, and malfunctioning of hardware.

PC Security Tools:

Windows Logon (Password and User Accounts), Local Security Policy, Windows Firewall, Antivirus, Security Settings in Internet Explorer,

Anti Spam and E-mail security, Windows Updates, Event Viewer.

PC Maintenance Tools:

Backup, Detecting and Repairing Disk errors, Disk Cleanup, Disk Defragmenter.

Thanks.

IMRAN GHANI
SR. SYSTEM PROGRAMMER
DUCC, UNIVERSITY OF DELHI
DELHI-110007

E-mail: ighani@ducc.du.ac.in
imranghani@hotmail.com
Web: http://people.du.ac.in/~ighani