Fast Track to Security

By Team Digit

Credits

The People Behind This Book

EDITORIAL
Deepak Ajwani Editor
Robert Sovereign-Smith Copy Editor
Ram Mohan Rao Writer, Copy Editor
Abey John Writer
Arjun Ravi Writer

DESIGN AND LAYOUT
Sivalal S, Vijay Padaya Layout Designers
Sivalal S Cover Design
Harsho Mohan Chattoraj Illustrator

September 2006
Free with Digit. Not to be sold separately. If you have paid separately for this book, please e-mail the editor at **editor@thinkdigit.com** along with details of location of purchase, for appropriate action.

Better Secure Than Sorry

The old adage goes "Better safe than sorry," of course. We'd change that to "secure" because of the sheer importance that word has taken on. What used to be money, gold and such is now data, and data cannot be secured using a six-lever padlock.

The purpose of this book is two-fold: to be an eye-opener, and to be a guide. It is our intention to tell you just how vulnerable you are, and we follow that up by telling you what you can do about it.

Admittedly, a lot has been written in *Digit* about viruses and other threats, but (a) we have tried to collate all such information into one handy reference, and (b) we have included here an anti-virus shootout. The biggest security-related threat out there is, of course, The Virus, and anti-virus software is, these days, something your personal computer can't live without. With that in mind, our anti-virus test will help you choose what's right for you. Anti-spyware tools have been discussed in depth as well.

Apart from viruses, adware, spyware, and other "wares", we also talk about how to keep data on your computer secure from other people. It's just a matter of good practice. You never know. And in some cases, it becomes a necessity—as in an office environment.

We also talk about how to keep your local network secure; about how to stay secure when on the Internet, in general; and about safety when on the move.

We should admit that much of what follows may seem to have been written for the paranoid, but paranoia is fast becoming a virtue.

Contents

Why Security?

Adware can bring down your PC, a virus can mass-mail annoying contents to all the contacts in your address book, a keylogger can send every keystroke of yours to someone on the Net—and these are just a few risks that are out there affecting PCs. Also, for someone even moderately well versed with operating systems, getting into a poorly-secured PC is child's play. We begin this *Fast Track* by telling you just how important security is.

As computers become more and more integrated into our lives, we end up leaving a lot of sensitive information on our PCs—from passwords, e-mail IDs (even official e-mail IDs) and bank accounts to personal diaries and notes, business plans (or worse still, tender bids), confidential documents, a log of surfing habits (which can be viewed out of context), a backup of phone SMSes, and much more.

Then there is another risk, especially when you are online—viruses and spyware. Though viruses and spyware are talked about in the same breath, there is one fundamental difference: a virus is written to cause damage to your operating system, programs or files, usually with no direct benefit to the virus creator. Spyware, on the other hand, is written for gain. This could be by tracking the surfing habits of a user on an infected computer and sending this information to someone who would send the user advertisements supposedly targeted at him based on his surfing habits.

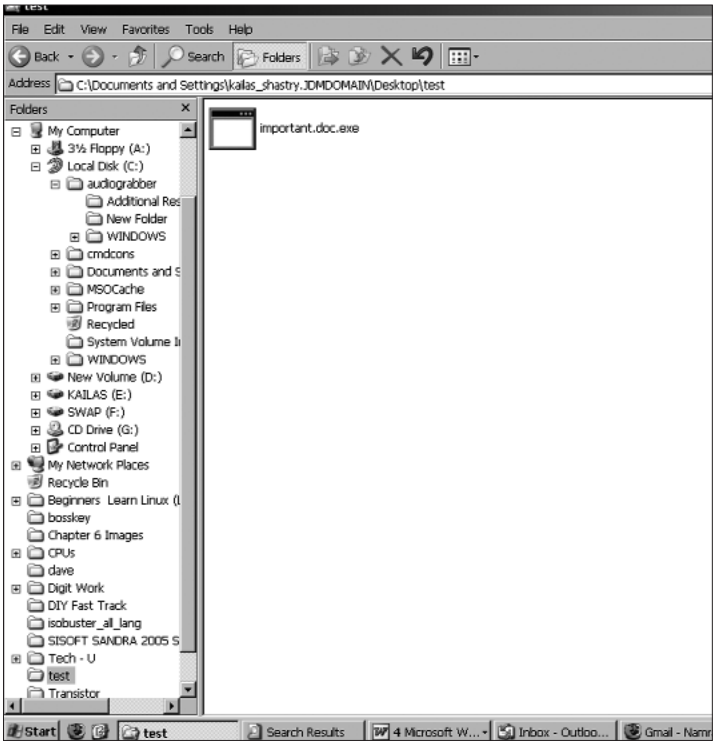
Very strictly speaking, spyware is not intended to cause damage, at least in the traditional sense, but more often than not, they end up doing so on your PC, which is rendered difficult to repair. You can find more details on viruses and spyware in the third and fourth chapter of this book.

When we speak of computer security, what we mean is the ways in which you can prevent people from accessing data on your computer, keep your computer safe from viruses and spyware, and protect yourself from hacking and phishing.

Let us take a brief look at the ways in which your security could be compromised. You will find more details on each of these in the respective chapters.

1.1 Floppies / CD / DVD-ROMs / External Storage Devices

Floppies have been the most common means of virus infection (especially if an infected file was used to boot the computer) during the time when they were common. Most viruses of that time infected the boot sector and occupied some of the 640 KB of memory that was used by DOS. Some notorious ones could delete files with certain extensions on a particular date. For some strange reason, the dates in most cases would be the 26th or 28th of a month. Though floppies are obsolete now, and viruses have evolved to do more advanced things than simply



Here's an example of an EXE file masquerading as a Word document

replicate themselves on floppies or hard disks—like mailing themselves to all your address book contacts, for instance—it is still a good idea to scan a floppy (when you must use one) for viruses after inserting it, if you haven't enabled real-time scanning in your anti-virus program. In fact, not enabling it is in itself a bad idea! Take the same precaution with CDs and DVDs as well.

The same precaution holds if you are opening or copying files from a hard disk you plugged in, or from an external storage device.

An oft-repeated tip is to avoid opening a suspicious-looking file. So just what does "suspicious" mean? Many a time, viruses disguise themselves to look like a common file type, such as using an MS Word icon to look like a Word document. The extension will be something like .doc.exe . Note that the ".doc" in the file name is not its true extension, but the ".exe" is (the characters following the last dot are the real extension of a file). So you can have "tech.abc.xyz.123.doc", and its true extension is .doc. Now why would a file try and look like what it actually is not? Only to fool you into thinking it's a safe file and make you open it—this is what you need to be wary about.

When accessing files from a CD or external device, enable showing of extensions in Windows Explorer by going to **Tools > Folder Options > View**. Here, uncheck "Hide extensions for known file types". Then if you come across a file with a jpg.exe, .doc.exe etc. extensions, avoid opening them. This holds good not only for accessing data from devices other than your hard disk, but also when you download a file from the Internet or check your mail for attachments.

Avoid downloading files with the following extensions if you are not absolutely sure that it is a file you need: EXE, ZIP, SCR, PIC, BAT, PIF, VBS.

1.2 The Internet

The Internet brings the world to your desktop, no doubt. But that world also includes a sub-world of spyware, worms, phishing attacks, and more.

The most common of online irritants is spam e-mail. Spam is simply unsolicited email that urge you to buy herbal concoctions to enlarge certain body parts, promise youthfulness via a pill, say that you've won a Rolex watch, and so on. These mails invariably contain a link to a supposed online store that will ask you for a credit card number for an online payment. It is difficult to believe how someone can fall for a trick like this, but apparently, there are a few innocent people out there who get tricked into buying a "herbal" cure or a "collector's watch." Needless to say, you need to just delete these mails.

The other common annoyance, which can also bring down your PC, is spyware / adware. The source of these is most usually pornographic sites or those with cracks for software. These sites can also be the very links you get in spam mail. Once they get installed, they are able to send a list of the Web sites you surf, and even your e-mail address. Based on your surfing habits, spam is sent to your email ID, advertising products or services that would ostensibly be of interest to you.

An adware program will open browser windows all by itself and direct you to Web sites selling products of the same nature. Some of them are so designed that if you close the window that they bring up, they will open two or more instantly!

If you receive a suspicious looking file in an e-mail (something like "annakournikova nude playing tennis.avi.scr") even from a known source, do not download the file. It is likely that a virus has hacked into the sender's e-mail client (or even disguised the sending address as something else—yes, that's possible too) and is sending out spam or offensive mails. The affected

person may not even know that spam mails from his ID are being sent. You can be a good friend and call him up to let him know of this so he can take curative measures.

Some sites even make use of the fact that people occasionally make typographical errors! A recent example is www.ork0t.com (now taken down), which you could have visited if you typed what you thought was "www.orkut.com" and made a typo. When one entered one's user ID and password into that site, it would be used to hack into your account and send out spam to all your contacts!

Phishing is a threat that can potentially rob you of your money. It's a means of fooling you into disclosing your login details of any site / service. If you are using an e-banking service, be very careful of mails that you may receive claiming to be from your bank, asking you to fill in your login details. As a policy, most banks do not send out e-mails asking you to fill in any e-banking details. If you do receive such a mail, it is fake. Before you fill out any details on a site following a link sent via e-mail, do confirm with your bank's customer care if they have indeed sent out such a mail. Visit only your bank's official site for all transactions.

1.3 Attacks From Known Sources

It is not uncommon for crime investigators to find that the culprit was known to the victim—this is the case with computer security as well. Someone who works at your computer may access your personal files—and even your surfing habits. It is not generally practical to keep your PC under lock and key, but what you can have is a digital version of a lock and key: set up passwords and encrypt files.

Data theft is a growing concern amongst corporates. Personal and professional harm can arise if someone gets access

to your private data or worse still, your e-mail, wherein they could email someone posing as you.

You can assign a password to access your PC and, similarly, password-protect your files as a first step to safeguard yourself from this risk. And, it is good practice not to let anyone install unfamiliar programs on your computer.

You must realise that given sufficient time and resources, a competent enough person can eventually break into your PC, but that is no reason to leave it entirely unsecured.

Thus far we have only taken a cursory look at common risks. In the coming chapters, we will talk about each of these and more in greater depth and the ways and means in which you can protect yourself from these risks. To reiterate, just as it is important to get a good lock and key for your house, it is important to adequately secure your PC in order to have a safe computing experience.

Securing The Desktop

Nearly 90 per cent of all PCs run the Windows operating systems—this makes Windows a victim of its own popularity. With more than three million lines of code, it is a given that vulnerabilities will exist in the operating system. Microsoft's security initiatives since Windows XP have done much to alleviate the problem; however, the fact remains that securing your desktop is still something *you* need to do.

2.1. Before anything else: patch, patch, patch!

New vulnerabilities are constantly being discovered. Depending on the nature of the threat and its severity, Microsoft regularly releases security updates and patches for affected operating systems and application software. To ensure that the security update or patch is applied as soon as it is available, turn on Automatic Updates. To do that, open the Control Panel, click on System, and select the Automatic Updates tab. Choose the first option to download the updates and get a notification when they are ready to be installed.

Turn on Automatic Updates

Other than operating system updates, Automatic Updates also downloads all high-priority updates for Microsoft Office XP, Microsoft Office 2003, Microsoft SQL Server, and Microsoft Exchange Server. Note that if you use older versions of Office products, you will need to visit the Office Web site (http://office.microsoft.com) for the latest updates.

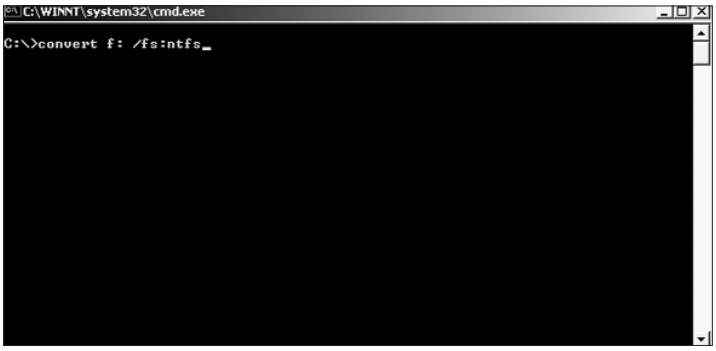
If you are interested, you can also subscribe to security bulletins via e-mail from Microsoft. These cater to both the home user as well as the technical professional. Go to **www.microsoft.com/ technet/security/bulletin/notify.mspx** and subscribe to your choice of security information updates.

2.2. Ensure disks are formatted with NTFS

NTFS is the recommended file system for Windows XP. It gives better access control protection for files and folders as compared to the FAT family of file systems. NTFS enables you to specify which users or user groups have access to which files and folders on your computer. You can also determine what the permission level for each user and user group should be. User permissions can be set to full control, change (cannot delete) or read only. It also gives better performance on hard disks that are larger than 32 GB in size.

To get a quick overview of the file systems on your computer, right-click My Computer and select Manage. Click on Disk Management in the left pane under the Storage section of the tree. The graphical view will show you all your hard disks and partitions, along with the file system they're currently formatted with.

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"**.



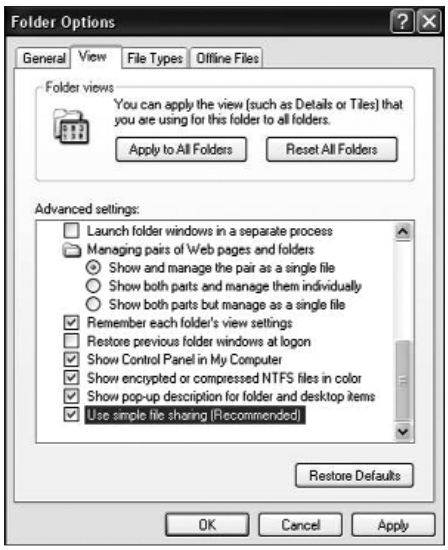
Convert your FAT or FAT32 drives to the NTFS file system

If you wish to see the details of the conversion process, turn on verbose mode using the /v switch. Note that this is a one-way conversion: you cannot undo the conversion once it has been done. Also, data loss is unlikely when you convert a FAT volume to NTFS, but it's still a good idea to take a backup before you convert.

2.3. Turn off file sharing

In Windows XP machines that are not part of a domain, files are shared using Simple File Sharing. For standalone home PCs that directly connect to the Internet, this is a potential security risk—attackers can enter your system through this route using an existing or currently unknown vulnerability.

To turn off Simple File Sharing, open My Computer, go to **Tools > Options**, select the View tab, go to Advanced Settings, and clear the "Use Simple File Sharing (Recommended)" checkbox.



Uncheck the 'Use Simple File Sharing' option

Note that if you are on a peer-to-peer home network, or if multiple people use the same computer with their own user accounts or the guest account, they will not be able to access any folders you want to share with them unless you use the advanced security options to configure access. To allow access to specific folders for specific users, right click on the folder,

select Properties, and click on the Security tab. You can configure the access rights for users and folders from this tab.

2.4. Use user accounts and passwords

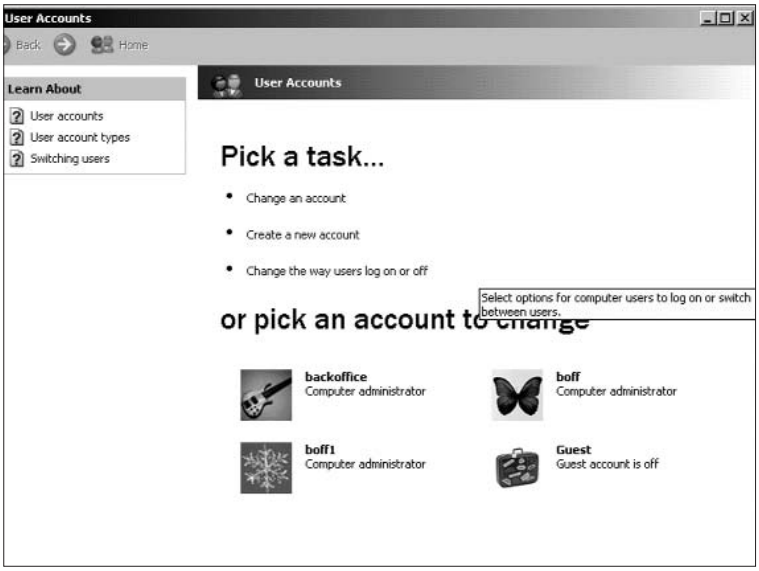
Assign user accounts and passwords to all regular users of your computer. Individual user accounts not only enables Windows XP to personalise settings for each user, it also enables one to control what users can access on the system. Thus, normal users will be unable to delete or change critical system files. Also, a good security practice is never to use blank passwords: that is an open invitation to attackers.

As a rule, if you are the primary user of your computer, set up two accounts for yourself: an Administrator account and a regular (limited) user account. Running your computer in Administrator mode and connecting to the Internet is a potential security risk, as Trojans or viruses that manage to enter the system will have complete access to the system with Administrator privileges. These malicious software can then wreak havoc on the system: they could format the hard disk, delete important system files, and so on.

If you require to do any system administration tasks like upgrading the system or changing the system configuration, log off from your regular user account and log back in as Administrator.

Assuming your computer is not part of a domain, log in to your computer as Administrator and go to *Control Panel > User Accounts*. The Administrator account allows you to do the following:

- Create and delete user accounts
- Create passwords for other accounts
- Change account names, pictures, passwords and account types



Use Windows XP's User Account manager to make sure that all your users have accounts and just enough privileges

The logged-in Administrator account cannot be changed to a limited account type unless there is at least one other Administrator account. This prevents users from accidentally (or intentionally!) locking Administrators out of the system.

Users of a limited or regular account cannot install software or hardware, and cannot change the account name or account type. These have to be done via an Administrator account. The regular account can, however, run software, delete the password (not recommended) or change it, and change the account picture.

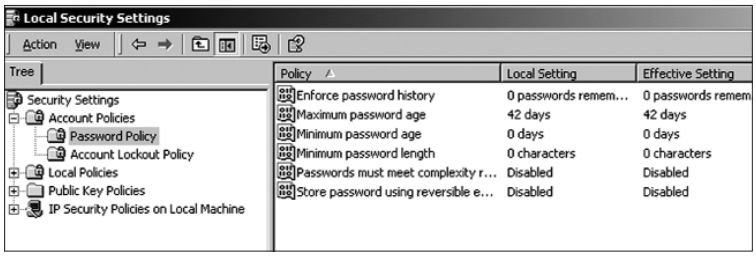
Some programs require that they be launched by the Administrator. For these applications, rather than logging in as Administrator, there is a Run As option, which can be invoked

from within a regular user account. Right-click the executable file that needs to be run in Administrator mode and select Run As.... In the 'Run As Other User' dialog box, select the "Run the program as the following user" radio button and enter the username and password for the Administrator account.

Note that for this to work, you would need to have the Secondary Logon Service running. At a command prompt, type in "services.msc", and verify that the Secondary Logon Service is running.

2.5. Strong password policies (XP Pro)

To ensure that all users of your system comply to a minimum set of good security practices, you can use the Local Security Policy console to set up security policies for your computer. Go to **Control Panel > Administrative Tools > Local Security Policy**. Expand Account Policies in the left pane and select Password Policy.



Password Policy Settings make sure all a computer's users are careful about their passwords

Set the following parameters to ensure that users obey the security policies in effect on your computer:

- Set the minimum password length to eight characters

❍ Set the minimum and maximum password age to an appropriate length of time—typically between 1 and 42 days. The password will expire at the end of the specified time, and the user will have to create a new password.

❍ Set the password history to at least six to prevent users from re-using the last six passwords. Home users need not be so stringent and can use a setting of three as well.

2.6. Use the account lock-out policy (XP Pro)

In XP Pro, a user account can be locked out after a specified number of invalid logon attempts. This can either be a genuine mistake by a user who has forgotten or mistyped the password, or an attempt by malicious software to crack the user account.

❍ Set the lock-out duration to 30 minutes. This will prevent users from logging into the system for 30 minutes after a specified number of invalid logon attempts. For higher levels of security, setting this to value to zero prevents users from logging in to the account right until the Administrator resets the password.

❍ Set the lock-out threshold to between 5 and 10 invalid logon attempts.

❍ Set the counter reset to between 5 and 10 minutes so that the count of the invalid logon attempts that do not reach the maximum are reset after this duration.

2.7. Mark personal folders with "Make Private" (XP Home)

Windows XP Home hides the complexity of the file sharing and permissions system of NTFS, but provides a useful feature to

limit access to folders from other non-administrator users. Right-click on a folder, select Properties, and set the "Make Private" option to protect your folders from unauthorised access by others.

2.8. Turn off or disable the Guest Account

If your computer is a standalone system that only connects to the Internet, you should disable / turn off the guest account—just so people you haven't given out your password to won't be able to access your computer. The Guest Account is also used to allow unauthenticated users from a LAN to access shared folders and files on your computer.

Go to **Control Panel > User Accounts**. To delete the Guest Account, just select it and hit Remove. However, it is better to disable it as there is a chance that you may require the account at some point in the future.

Select the Advanced tab and click Advanced. In the "Local Users and Groups" window, select the Users branch of the tree in the left pane. Right-click on the Guest Account and select Properties. In the resulting dialog box, select the "Account is Disabled" checkbox. The Guest account will no longer be accessible for logging on either locally or from another computer on the network. Note that this procedure may vary slightly for Windows XP Home.

2.9. Delete / Disable Unused User Accounts

Earlier, users of your system may have left their accounts on the system. This can be another avenue for potential security compromise—if these users gain access to your system and use it for a malicious purpose. If the users are temporarily not using their accounts, disable them, else delete

them by following the procedure outlined for the Guest Account above.

Note that some software installations will create a user account for their own purposes. For example, installing the .NET Framework will create an user account called ASPNET. These types of accounts are system accounts and should not be modified or deleted unless the associated software has been removed or is no longer needed. Normally, uninstalling the software should also remove the account.

2.10. Disable unnecessary services

When Windows XP starts, a number of programs start as part of the core operating system. These are generally known as "services". Typically, Windows XP will also have a number of services that are non-critical but running in the background, consuming system resources. There is also a potential security hazard as these services, especially the lesser known ones, could have some as-yet undiscovered vulnerability which could be exploited. Disable all but the most essential services.

To view the list of running services, type in "services.msc" at a command prompt. Click on the Status column heading and sort the list to view all running services. Some viruses and Trojans sneak into the system and install themselves as legitimate-looking services. Review the description of each running service to get a basic understanding of what it does. You can selectively stop a service, set it to start Manually (when invoked by another program), Automatically start with Windows, or Disable it entirely. The following services are typically safe to disable:

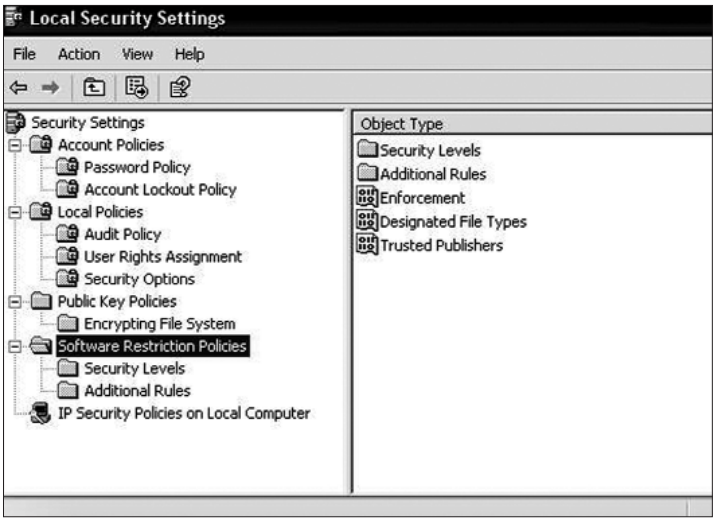
- Telnet
- Universal Plug and Play Device Host
- IIS (not installed by default)
- NetMeeting Remote Desktop Sharing
- Remote Desktop Help Session Manager

- Remote Registry
- Routing & Remote Access
- SSDP Discovery Service

If you see a suspicious-looking or blank-description service, investigate it by double-clicking on the service and opening its properties sheet. The file name and path to the file will be shown in the "Path to executable:" field. Go to the location where the file is located and right-click on it to see its properties. For Microsoft system files, a version tab should also be available, which gives a good indication of its origin. If the file is suspect, update your virus and anti-spyware definitions and scan the file.

2.11. Set software restriction policies

You can control the software that can be run on your computer by configuring the Software Restrictions Policies in the Local Security Policy (**Control Panel > Administrative Tools**).



Software Restriction Policies

By specifying which programs are authorised to run on your system you ensure that only those programs are allowed to launch. Any attempt by any other program to start with or without the user's knowledge will be unsuccessful.

2.12. Securing the Linux Desktop

Linux has acquired a reputation for being "virus-free" and more secure than Windows. However, vulnerabilities do exist, and Linux, more often than not, is not optimally configured for the home user. Thus, home users will need to close off some of the potential vulnerabilities manually.

Standard Linux installations will have many services that are started with the operating system. These, in most cases, are useless for the home user. For example, the FTP service runs an ftp server that is used to transfer files to and from the PC. This is not required on home PCs as home users will be primarily downloading files. The FTP service is useful if you are storing files that are downloaded by a large number of users. Similarly, the SMTP service is an e-mail service that is not required on most home PCs. The programs that run these services are known as daemons. These daemons run in the background waiting for some event to occur to respond to. To secure the Desktop, disable all unnecessary services from starting when the system boots up.

Inetd

Inetd is a super daemon that controls a number of network daemons. You will need to modify the configuration file inetd.conf to disable all unnecessary services. Open the inetd.conf file, normally found in the /etc folder, in a text editor like pico. To do that, open a terminal window and type "**pico /etc/inetd.conf**". Scroll through the entries looking for listings like:
ftp stream tcp nowait /usr/etc/in.ftp in.ftp

If your computer received an FTP request from another computer, inetd would use this line to start the FTP program. Comment out this line by putting a hash (#) at the beginning of this line. Similarly look for other entries similar to this one for telnet, finger, shell, login, talk, ntalk, and auth. Press **[Ctrl] + [X]** to exit pico. When prompted to save the file, press **[Y]** and hit **[Enter]**. You will now need to restart Inetd to let the changes take effect. At the command line, type killall -HUP inetd to restart inetd.

Other Services

There will most likely also be other useless or potentially risky services running on your system apart from those listed in inetd. These include apmd, atd, netfs, httpd, portmap, pcmcia, nfs, sendmail, routed, rstated, ruserd, rwhod, and ypbind. These could allow a savvy Linux hacker to gain access to your system and take over as the system root using some known or currently-undocumented vulnerability in any of these services. The concept is to provide the *minimum footprint for an attack vector*.

You can manually disable these services by renaming the associated program file for each of these services. To do this you would need to know the runlevel of your computer. Linux has six runlevels that load different services at startup. If you are booting into a command line environment, you will usually be at runlevel 3. In a GUI environment, the runlevel is normally 5. To find out your runlevel, type in "runlevel" at the command prompt. This will display the current runlevel of your computer. You will now need to change to the specific runlevel directory to disable the service from starting up at boot.

On Red Hat systems, type in **"cd /etc/rc.d/rc3.d"** (or **"rc5.d"**) depending on whether you are in runlevel 3 or 5.

Type ls at the command prompt to list all the files in the directory. If the file name begins with S, it is set to automatically start with the operating system. For example, in the

directory **/etc/rc.d/rc3.d**, there may be a file called **S60nfs**. This starts the nfs service at runlevel 3 when the operating system starts. To disable this service, rename the file by typing in "mv S60nfs K60nfs" (Red Hat uses the K prefix to indicate disabled services). Similarly, review the files in the other runlevel directories to disable unwanted services from starting up.

Virus Busting

In this chapter, we get into the nitty-gritty of the virus menace, for lack of a less clichéd phrase. And, well, "menace" is quite a good word for the problem, anyway. What are the warning signs? What anti-virus to use? Is Linux as safe as it's touted to be?

3.1 How To Tell

So how do you decide that the battle has begun and that a full system scan is in order?

Whether you love your computer enough to have given it a name or whether it's someone else's property that you just work at, you know your computer best. It's easiest for *you* to tell if your computer is infected. The keywords: "odd behaviour." If you say to yourself, more than five times a day, "Now how did *that* happen?"—you're probably infected. Actually, there's one more question on that list: "Why is this thing so *slow*?"

Having said that, we need to decide on what "slow" and "odd" mean. First off, whatever your machine, you know when it's running slower than usual, and when that happens, there's a possibility that you're infected. Windows pop up more slowly. Random activity seems to be happening in the background more often than it should. Something negative seems to have happened to the overall responsiveness of the system.

One thing to remember is that slow behaviour could also be due to spyware, and it doesn't necessarily mean a virus. Of course, it could be nothing at all, and all in your head.

If you're using a firewall such as Zone Alarm, which tell you what program is trying to "act as a server" or is trying to "access the Internet," note the names of those programs. If you think they shouldn't be asking for access, you might be infected. But remember that lots of programs these days try and update themselves automatically, so there could be several false alarms. Reduce these by turning off automatic updates on all your programs, though that might mean looking through a lot of menus. If some programs are still asking for access, The Bad Thing might just have happened to your computer.

Then there's the System Configuration Utility, activated by typing in "msconfig" at a command prompt. Run it and take a good,

hard look at all the programs running. If you see something with random character strings as its name... you've guessed it: you're infected by either a virus or spyware. But most viruses and spyware don't give themselves away so easily, and call themselves by decent names.

Talking about running the SCU, if the SCU, the Registry Editor, or your anti-virus program itself doesn't load, you're almost certainly infected.

Keep in mind that a combination of symptoms is much more likely proof that you're infected: rarely does a virus have just one effect. That said, here's a checklist of what to look out for before you press the almighty Scan button on your anti-virus (if the virus hasn't already disabled it!).

0. Your computer takes charge and does things on its own—moving the mouse cursor all by itself, randomly closing and opening windows, showing you messages that say "We've got you!" and so forth. If any of this is happening, we don't even need to tell you that you're infected!

1. Your computer often stops responding. This is more so a sign of an infection with Windows XP than with earlier versions: Windows 98 used to stop responding often even without infection, so that doesn't mean much!

2. The crashes-and-restarts-on-its own syndrome: this is a pretty good indicator of viral activity on your computer. Of course, it *could* be something else, but if this is happening and your anti-virus is working, why not do a scan anyway?

3. Several apps seem broken. The key word here is "several": one program not working correctly, like we said, is seldom an indicator of a virus. But if you notice functional anomalies in several applications, it's time to scan.

4. Certain drives on your computer have suddenly become inaccessible, even though they show up in My Computer.

5. Not being able to print correctly has been stated as an indicator of a viral infection, but don't panic if you get a bad printout. It's probably due to something else. But if it happens in conjunction with other symptoms...

6. Unexpected error messages with weird codes! Of course, error messages are seldom user-friendly, so the key here is how often they pop up, and how weird they are. For example, a big red cross and an OK button that doesn't say "OK".

7. Now this is so typical of possible viral infection that we hardly need to mention it: distorted dialog boxes and menus. Hit "Scan" immediately. And if it turns out not to have been a virus, there's still something wrong with your computer, so have it checked.

8. If, despite all our warnings in the past five years, you still opened a suspicious-looking attachment—driven, of course, by what is called the libido—and immediately after that, everything (or at least some things) went funny, you're in for it. Hit Scan. And hope that the anti-virus *will* scan.

9. It could be that your anti-virus needs a re-install, but it's unlikely: if the anti-virus is disabled and you didn't disable it, you're very likely infected. Before panicking, first try reinstalling the anti-virus. If that doesn't work, panic.

10. Continuing along those dire lines, if you're able to install any program *but* an anti-virus, then yes, you are a victim.

11. When someone tells you he or she got an infected message from you, you almost certainly have something bad on your computer. It might or might not be a virus.

12. A not-so-common symptom, but a deadly giveaway, is the

mouse pointer changing to something else. Of course, if you went to one of those "1000 cursors free!" sites and downloaded and installed cursors, then you're infected by spyware anyway.

13. Icons on the desktop that you didn't place are again a giveaway symptom.

14. If you just installed a program—successfully—and it doesn't work properly, or if its icons have vanished, don't reinstall it! There's no time to waste—quickly do a scan.

15. Now this could also be an indicator of spyware, but when you notice that your modem is doing a lot of activity on its own—both sending and receiving—or if your hard disk is performing more activity than you'd expect, like chattering away when you're not even working on anything, it could be a sign of viral infection.

3.2 Enter The Warriors

It's time to take a look at your trusty system-tray defenders, the anti-viruses themselves. We did say in the previous section that you'll need to scan your computer if you noticed any of the symptoms we described, but now the question is, what anti-virus to choose?

There are two aspects to an anti-virus—one is its resident protection feature, that is, the feature by which it constantly monitors your system for suspicious activity. The other is the option whereby you scan areas of your computer for infection. All the anti-viruses we'll be talking about have both these.

In the case of anti-spyware scans, you can run a scan using one program and then repeat it using the other, so each catches what the other missed. But unfortunately, you can't have two resident anti-viruses: they'll conflict with each other. As a result, you'll have to decide upon one. The following test will help you do so: it's

a full-fledged test we conducted on several anti-virus solutions, both free and paid.

3.2.1 How We Tested

All the anti-virus solutions were tested individually on a fresh installation of Windows XP Professional SP2. The test machine comprised an Intel Pentium 4 3.2 GHz processor with 1 GB DDR2 RAM and a Maxtor 120 GB 7200 RPM SATA hard drive. We installed the latest updates for Windows XP and the latest drivers for hardware, as well as DirectX 9.0c.

We noted the initial boot-up time of the test machine and the increase in boot-up time after the anti-virus software was installed. We restarted Windows twice to make sure that all the services installed by the anti-virus were up and running. We thoroughly scanned the entire hard drive and noted the time taken to complete the scan process. We noted the page file usage of the clean system and then noted the memory usage after the anti-virus was installed, then once again during the test scan. The average CPU usage during the test scan was also noted.

We obtained the virus scanning scores of individual anti-virus software from www.av-test.org and compared the test results head-to-head. Since the virus detection rate was almost 100 per cent for these solutions, we compared the average response time of the companies in case of virus outbreaks.

The response time to a virus outbreak is of prime importance because it determines the time period for which the computer remains vulnerable to attacks from a new virus. It is the average time taken for the anti-virus to receive the update required to protect your computer against the new virus.

In addition to performance, we also noted and rated various important features. We noted the number of clicks it takes to initiate a virus scan. We also noted whether features such as heuristic scan, e-mail scan, rescue disk creation, installation size

requirement, and so on. If the anti-virus came bundled with a firewall, it was given extra points. The automatic update feature was also given points if present.

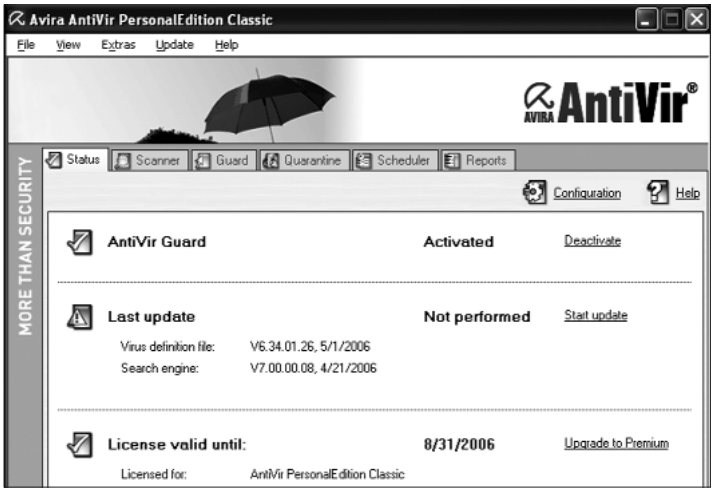
In addition to these, we also noted if the vendor posted downloadable virus definition updates, the frequency of these updates, and also whether outbreak alerts were posted on the Web site. Telephone support and toll-free support was also awarded points. Last but not least, the price of the anti-virus (in the case of the paid ones) was also considered to decide our winner.

3.2.2 Free anti-virus software

3.2.2.1 Avira AntiVir PersonalEdition Classic

Avira AntiVir PersonalEdition Classic is a free anti-virus solution for home users. During the installation, the user has the option to install either one or both modules: AntiVir Guard and Shell Extension.

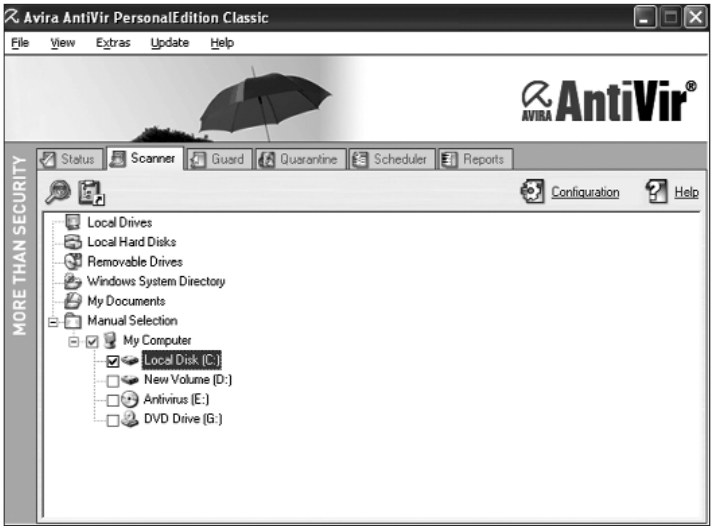
The AntiVir Guard is the on-access scanning element of the software. It runs in the background and monitors files during



The AntiVir interface is very simple and easy to navigate

operations such as open, write and copy. When a user operates on a file, AntiVir Guard automatically scans the file for infection. The Shell Extension module installs a new menu item to the right-click context menu. This way, you can conveniently scan any file or folder by just right-clicking on it.

The interface of the software is easy to use and one can feel right at home using it. Interestingly, the main window doesn't



Scanning drives with AntiVir

show a button to start a scan. You can either trigger a scan by using the right-click menu or by dragging and dropping a file or folder onto the window. As it is the main window of the program, it only shows buttons to configure the anti-virus program.

Avira AntiVir PersonalEdition Classic supports scanning files compressed with almost all the major file compression formats. There is also an option to scan only the boot records; this is useful if a boot sector virus has infected your computer.

The software is light on system resources and increased the boot-up time by just 7 seconds. It also logged the lowest scan times of 231 seconds in our test scan. While scheduled scanning is supported, e-mail scanning is absent. The outbreak response time of this anti-virus is between four and six hours, which is somewhat comfortable for the user as it leaves the system vulnerable for not very long. You can upgrade to the Premium version for just Rs 1,200 and get additional features such as MailGuard, adware, and spyware detection.

Web site: www.free-av.com/index.htm
Minimum System Requirements: Windows 98 or higher, NT or higher (not Server), 128 MB RAM for Windows 98/ME/NT, 196 MB RAM for Windows XP, IE 5.0

3.2.2.2 avast! 4.7 Home Edition

When we installed and fired up this anti-virus for the first time, we were left wondering whether we had accidentally launched a media player instead. Avast! has the looks of a media player; it even has interface elements that resemble the volume control dial and the play button. What's more, the interface is skinnable. Beneath all the flashy looks, though, beats a reliable anti-virus engine. You can scan your PC with just two clicks, and if you need to scan a particular folder, it is achievable in no more than four. The context menu can also be used to do this.

The snazzy avast! interface is easy on the eyes

After installation, we needed to restart Windows, when it performed a boot-time scan. Incidentally, such a bootup scan can be scheduled to run each time Windows boots. It even supports scanning files being transferred using P2P agents and instant messengers.

This anti-virus has a unique feature known as VRDB or the "Virus Recovery Database". What the VRDB does is, it creates an integrity database of essential files on your computer; that is, it stores information about the state of the files, creating as many as three versions for each file. The VRDB is created either when the computer is idle or upon request. Through the VRDB, if a file is infected, it can be quickly restored to any of these three versions!

avast! 4.7 Home supports e-mail scanning for clients supporting SMTP, IMAP and POP3 such as MS Outlook, MS Exchange, Outlook Express, Eudora, Pegasus Mail, Netscape Mail, Mozilla Mail, and IncrediMail. It can clean many adware and spyware, and can be updated automatically. It is also not too heavy on system resources.

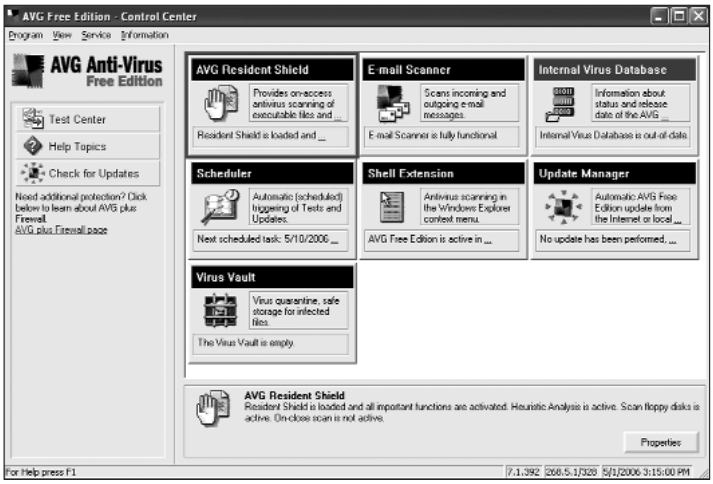
We must state here that it increased the bootup time of our test machine by 12 seconds, which cannot be considered too little. The outbreak response time is between 8 and 10 hours—a mediocre showing. A complete scheduled scan is not supported, and you cannot selectively scan only executable files if you wish to.

Web site: www.avast.com
Minimum System Requirements: Windows 9x/ME/NT/2000/XP/x64 (not Server), 64 MB RAM for Windows 2000/XP, 50 MB of hard disk space, IE 4

3.2.2.3 AVG Anti-virus Free Edition

The AVG Anti-virus Free Edition is free for private, non-commercial, single home computer use. After installing the anti-virus checks for updates for virus definitions and prompts you to create rescue diskettes. A rescue disk can be the lifeline of your computer if it gets infected by a virus and refuses to boot. You can either make use of standard 1.44 MB floppy disks or simply save the recovery data to the hard drive and later burn it to a CD.

The interface of the AVG Control Center is not well-designed. Especially when other anti-virus solutions have put in so much



The AVG interface is a little different from most others

work in pepping up their interfaces, the interface of AVG seems dated. Nevertheless, it lets you configure the programs' modules, which are AVF Resident Shield, E-mail Scanner, Internal Virus Database, Scheduler, Shell Extension, Update Manager, and Virus Vault. There are sections for each module which let you view information regarding that module and also configure and use them. You can configure standard features such as on-access, context-menu, e-mail, and scheduled scans and also check and update virus definitions. But we have to admit that even though it is clumsy, the interface still does get the job done.

In the opening screen of the Control Center, you need to click just once to start scanning your computer and three to scan a particular folder, which is very good. There are three predefined scan types:

1. "Complete Scan" in which all the local hard drives are tested.

2. "Selected Areas Test" in which you can scan disks, directories, removable devices, and other areas that you specify.

The three types of scans are clearly visible in AVG's interface

3. "System Areas Test" in which only important system areas, files and registry keys are scanned.

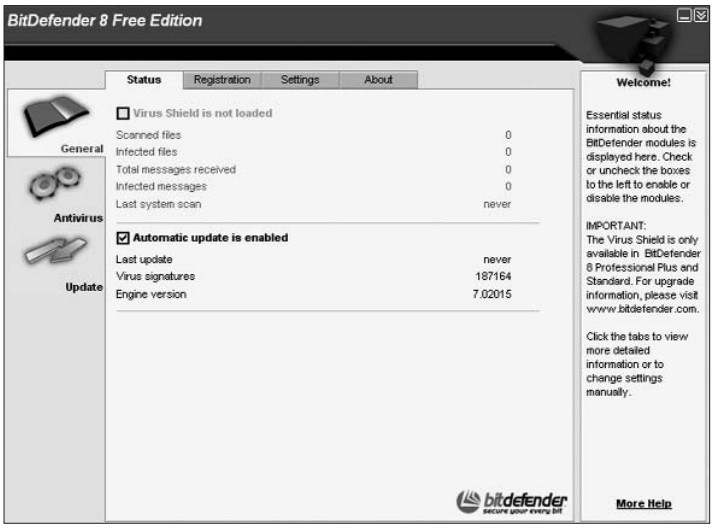
E-mail scanning is supported and integrates with e-mail clients such as Outlook, Eudora and The Bat!, you can also manually configure other e-mail clients. You can add virus-free notification to e-mails and can configure it to delete all or specified file attachments. The software also uses heuristic scanning and also blocks password-protected archives because it is not possible to scan within such archives without a password.

It increased bootup time by 14 seconds, and the average CPU time it consumed while running a scan was 28.9 per cent. It did not hog too much of available memory. AVG's response time for outbreaks averaged between 8 and 10 hours, and a lower time would certainly be desirable.

Web site: http://free.grisoft.com
Minimum System Requirements: Windows 9x/ME/XP/NT/2000, 32 MB RAM, 20 MB hard drive space, IE 5.01

3.2.2.4 BitDefender 8 Free Edition

BitDefender 8 Free Edition has a very simple interface that allows you to access the basic functions. This anti-virus has one big negative; it does not come with on-access protection. Not having an on-access scanner leaves the computer vulnerable to viruses even though the anti-virus is installed and you will need to run a manual scan to check for and get rid of any virus. The on-access scanner is available only in the Professional version which you'll need to purchase.



The lack of on-access scanning loses BitDefender points, big time!

Automatic updates of the virus definitions and engine is supported. Manual virus scanning is customisable. You can choose the drive or folder that you wish to scan. In addition, you can choose the type of files that you wish to scan such as boot sector, files, Mail Database, Archives and Packed files. You can also specify a file mask for files to be scanned, such that you can scan just executables or you may specify the file extensions that are to be scanned.

Heuristic scanning is supported, and hence newer viruses that might not be listed in the virus database can also be detected. You can specify the action to be taken when a virus is detected, such as whether the file should be deleted or quarantined or a user intervention be requested. It puts a significant load on the processor while scanning, it logged 44.25 per cent usage which is quite high; you may be unable to work while scanning is in progress.

Though it was not the fastest scanner, it wasn't too slow either; the test scan took 323 seconds, a little over five minutes.

BitDefender sported a commendable lowest average outbreak response time of between 2 and 4 hours, which leaves the system vulnerable for very little time.

There is no telephone support, but there is Live! Support, which lets you chat online with experts to try and find a fix for your problem.

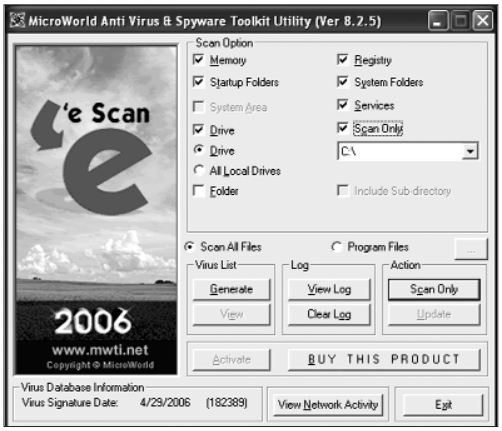
Web site: www.bitdefender.com
Minimum System Requirements: Windows 9x/ME/XP/NT/2000, 64 MB RAM, 40 MB hard drive space

3.2.3 Paid Anti-virus Software

Why would you want to pay for anti-virus software when you can get it for free? The short answer is simple—added functionality, and the permission to use it in a commercial setup. Paid anti-virus packages are usually complete security suites. As for the long answer, you'll have to read on to find out. Here, we take a look at some well-known and trusted anti-virus suites.

3.2.3.1 eScan Internet Security 2006

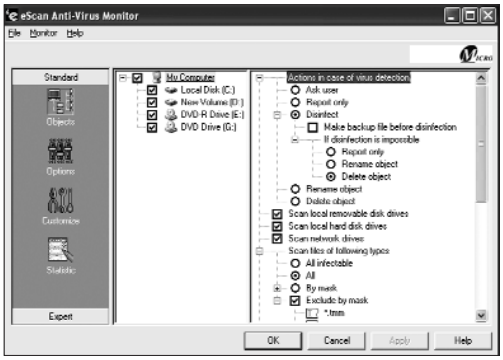
MicroWorld Technologies, Inc.'s eScan Internet Security Suite 2006 is a complete security suite that is based on MWL technology. MWL or MicroWorld WinSock Layer is a concept that allows for scanning Internet traffic in real-time.



The eScan interface is neat and clean

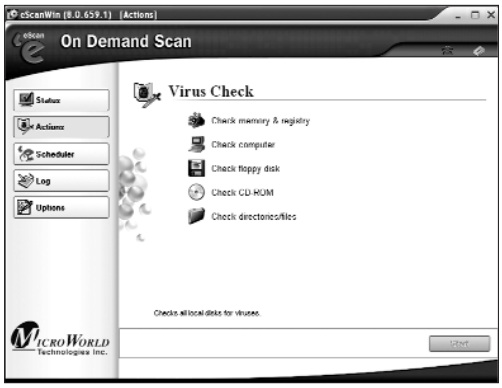
Traditionally, all incoming and outgoing mails pass through the WinSock Layer at both the client and the server level. The MWL sits on top of WinSock. Hence, all the content that passes through WinSock has to pass through MWL, where it is checked for malicious content. The checking is done by passing the data through various filters such as Virus Filters, Content Filters, Attachment Filters, and so on. An appropriate action is taken either using user intervention or automatically, in accordance with your setup. MWL thus potentially tackles a threat before it reaches your applications.

The eScan suite consists of eScan for Windows, eScan Content Administrator, eScan Auto-Updater, and more. The eScan for Windows module is the main program and it is from here that you can manually scan your computer and can set the scanning options. eScan Content Administrator is used to configure various elements

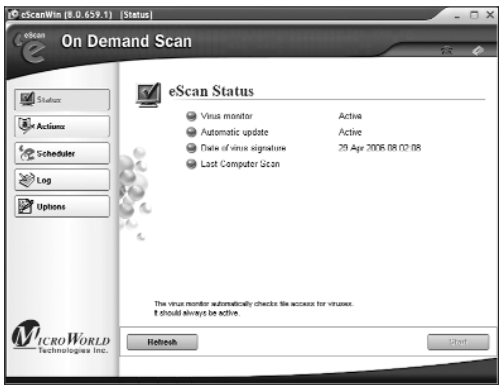


Scanning drives with eScan

such as e-mail content scanning, popup filter, Browser CleanUp, etc. There is also a program called "Quick Scan your system", which is another way to manually scan your computer but with customisation options. The module does not allow one to select whether or not to scan compressed files.



eScan's On Demand scanner...



...and the scan status

eScan Updater allows you to update your antivirus, Content Administrator lets you set security policies to permit or prohibit specific type of content from bring accessed (similar to parental control), and the eScan Management Console allows you to remotely configure and administer the eScan network when installed on multiple clients.

Heuristic scanning is supported, and so is scanning of archived and packed files. You can even opt to scan just the Registry or services. It supports spam blocking and also scans e-mails received on various clients such as Outlook Express, Outlook, Netscape, and Eudora. The Browser CleanUp feature protects your privacy online

by removing traces of Web sites that you have visited, and also allows you to remove cookies, ActiveX controls, plug-ins and other links that reveal your browsing habits.

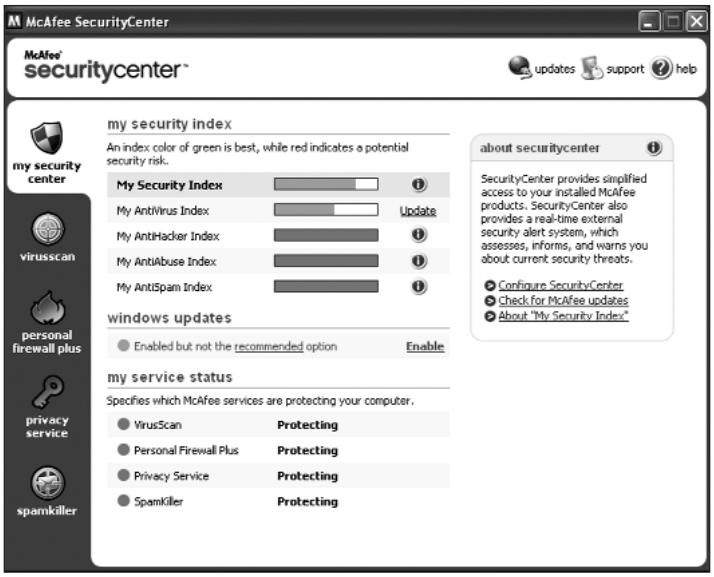
While scanning, we found that it exhibits an astoundingly low average CPU usage—just 1.62 per cent. Its memory footprint while scanning is quite high though at 325 MB or 75.68 per cent. But it took the longest time to scan—over 32 minutes. The increase in bootup time was just six seconds which is quite low. The on-access level of scanning for files and e-mails can be changed just by accessing the system tray icon. According to the database from **www.av-test.org**, eScan Internet Security Suite 2006 has a fast average response time of just 2 hours in case an outbreak occurs, which is an essential plus point of this anti-virus.

Web site: www.mwti.net
Minimum System Requirements: Windows 9x/NT/2000/XP, 64 MB RAM, 50 MB free hard disk space.

3.2.3.2 McAfee Internet Security Suite 2006

McAfee Internet Security Suite 2006 consists of SpamKiller, VirusScan, Privacy Service, and Personal Firewall Plus; it is thus a comprehensive security suite. The interface of the software is clean and the set of utilities that it exposes is also extensive. Installation is swift and requires a restart. The user is asked to set up a password to access the McAfee Security Center. The main screen shows bar graphs of indices of Security, Anti-virus, AntiHacker, AntiAbuse and AntiSpam, which in general shows the level of security of the computer. Status of various services such as VirusScan, Personal Firewall Plus, Privacy Service, SpamKiller, as well as the Windows Update are also visible on these screen and can be enabled from here.

The WormStopper and ScriptStopper modules block suspicious behaviour within e-mails and scripts respectively. The SpamKiller module filters any POP3 account, regardless of the e-mail client used. It integrates nicely with Outlook and Outlook Express in the



The McAfee Security Center

form of a toolbar. The user has the option to hold the mail in a quarantine area within SpamKiller, or to mark its subject with the word “SPAM” and pass it on to the e-mail client.

The firewall module can be configured to handle inbound and outbound transfers of data. There is an internal database of over 4,000 programs that it identifies as ˜bona fide˜ programs and automatically allows network access to these. The new gaming-suspend mode suspends confirmation pop-ups during full-screen gaming sessions. If Personal Firewall detects intrusion attempts or suspicious activity during gameplay, the attempts will be blocked and you will be notified and prompted whether to grant access, after you exit the game.

The Privacy Service lets you store private data such as credit card numbers in a categorized and encrypted database. This service prevents sensitive data from going out via e-mail, an instant

messenger, or a Web form. When a program or user attempts to send across private information over the Internet, Privacy Service detects it and replaces the data with MFE, which is McAfee's stock symbol. There is also a File Shredder utility that lets you securely delete any confidential file from your computer forever!

The rescue disk option is useful in creating bootable diskettes which can be used to revive your computer in case of a virus infection that does not allow your system to boot.

This software is a resource hog, and generally makes for a sluggish system. It increased the boot time by around a minute. In fact, the system came to a complete standstill for some time after booting into Windows each time. Its memory consumption is quite high, though not the highest at 74.59 per cent while scanning, it logged a high CPU usage of 42.84 per cent while the virus scanning was in progress. A virus scan took 12 minutes to complete. The average outbreak response time was 10 hours which is rather high.

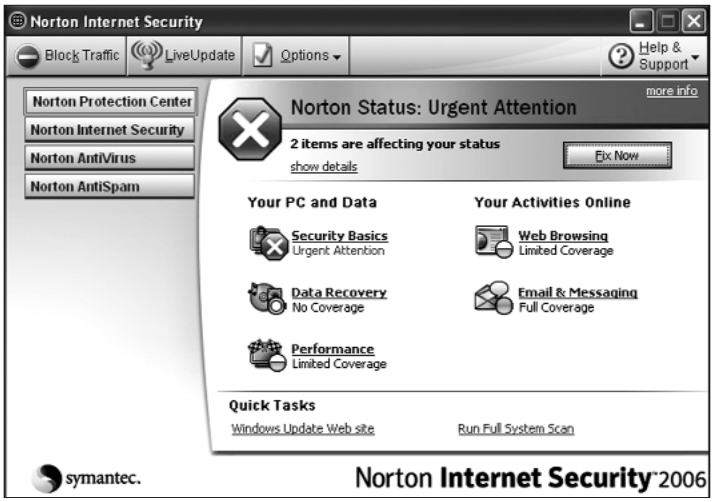
Web site: www.nai.com
Minimum System Requirements: Windows 98/ME/2000/XP, Pentium 133 MHz, 64 MB RAM, 100 MB hard drive space

3.2.3.3 Norton Internet Security 2006

This is the latest version of the popular Internet security suite from the Symantec stable. The interface of Norton Internet Security 2006 is almost like its predecessor, NIS 2005—neat, eye-catching and easy. Immediately after you install it, you are asked to update the software using its LiveUpdate utility which downloads program updates from Symantec's server. You can also download the virus definition files if you need from **www.symantec.com**.

We immediately noticed the Norton Security Center which appears as a toolbar beside the system tray. This notifies you of potential security threats to your system and also suggests actions needed to overcome them.

There is also a new Auto-Protect Spyware Blocking feature that

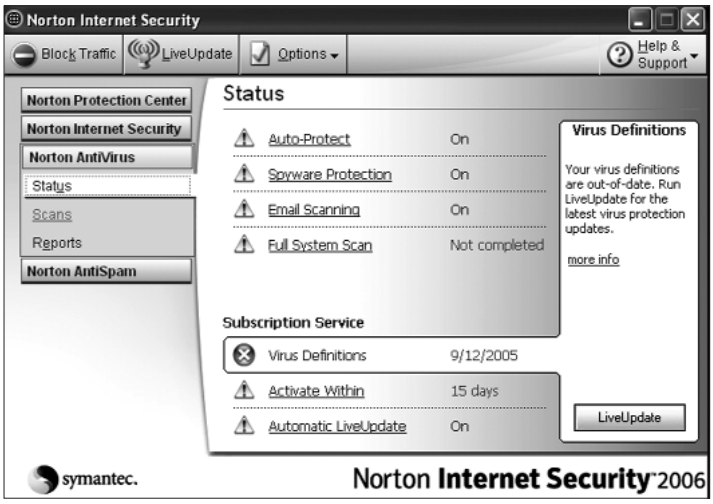


The Norton Internet Security Interface

improves the ability of NIS to block spyware, ad-ware, key-loggers, and other malware during installation. The Security Inspector finds, and in some cases patches, potential security holes, including weak browser settings and Windows passwords. For example, our test bed's Windows XP was not password-protected. Security Inspector detected this and suggested that we set a password of at least eight characters with at least one numeric character.

The Norton Home Page Hijacking Protection feature prevents rogue applications from changing your browser's home page to their own. Then there is Norton Firewall which is intelligent enough to form rules about which programs it should allow Internet access to, without needing the user's intervention.

Like its predecessors, the program also features a heuristic scan, or Bloodhound as Symantec calls it. A heuristic scan allows the program to detect an unknown virus, just from its suspicious activities. It works on the principle that viruses usually use documented tricks or methods of infecting, and if a file is found to



Updating NIS, and the way it informs you

behave in a similar manner, it is detected as virus-like.

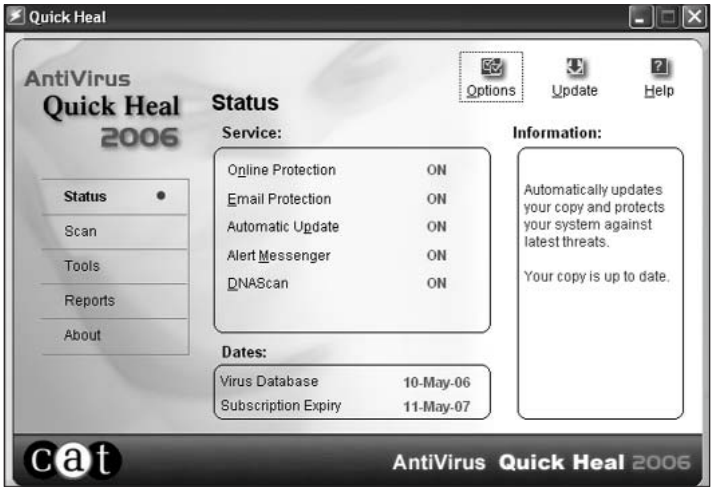
E-mail scanning is supported for incoming and outgoing e-mails for clients such as Microsoft Outlook Express and Eudora. Chat messengers such as mIRC, Pirch, ICQ, NetMeeting, Internet Phone, Net2Phone, and CU-SeeMe are also supported.

Norton Internet Security does require the highest memory resources; we found that it required 341 MB or 84.32 per cent of installed memory while scanning, while the idle memory consumption was 60.54 per cent, which is quite high. The CPU time it takes up averaged at 22.35 per cent. It took about 7 minutes to complete the test scan, which is quite fast. The average response time of Norton Internet Security 2006 is between 10 and 12 hours—one of the slowest response times amongst the products that we've tested.

Web site: www.symantec.com
Minimum System Requirements: Windows 98/ME/2000/XP, Pentium 300 MHz, 128 MB RAM, 40 MB hard drive space

3.2.3.4 Quick Heal Anti-virus 2006

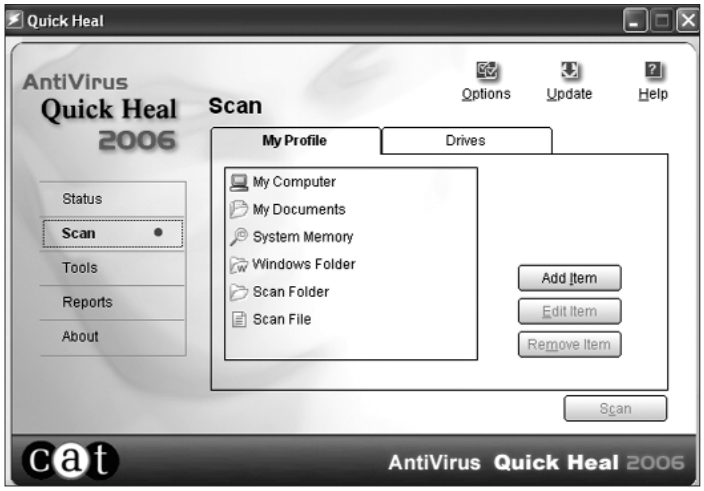
Quick Heal Anti-virus is manufactured by Cat Computer Services P. Ltd. of India. Installation was quite easy and requires one to obtain a license key file by registering online at **www.quickheal.com**. There is also an option to register offline.



The QuickHeal interface

The user interface is well done and easy to use. You just need three clicks to start scanning your computer, and if you want to scan a particular folder, it just takes a couple of clicks more. You can also schedule a one-time, daily or weekly scan. Scans can be also scheduled to run at predetermined time intervals.

Quick Heal's online or on-access protection loads at Windows startup and continuously monitors your computer for any malicious activity. Its e-mail protection watches out for and protects against viruses received in e-mails and attachments, e-mails containing vulnerabilities such as MIME, IFRAME, etc. It only allows known or trusted e-mail clients to send and receive e-mails, thus preventing worms from sending e-mails. Some of



Scanning hard drives with QuickHeal

the trusted e-mail clients are Outlook, Outlook Express, Eudora, and Netscape Navigator.

The scanner can be configured to scan only executables, all files or files with a specific extension. DNAScan, which is Quick Heal's name for a heuristic scan, can scan for unknown viruses, and the company claims that it has reduced the percentage of false alarms. Once an unknown virus is found, you have the option to try to repair the infected file, quarantine it, or submit it to the research labs for further analysis. You can use the Automatic Update feature to keep your anti-virus up-to-date.

While scanning for viruses in our test scan, we found that for the first couple of minutes or so, QH scan uses a lot of CPU time—as much as 90 per cent. But later on this drops to acceptable levels so that you can continue working. It also eats up quite a lot of memory during virus scanning, which we found averaged at around 335 MB, or 81.08 per cent. According to the data we acquired from **www.av-test.org**, the outbreak response time for Quick Heal Anti-virus 2006 is between 4 and 6 hours, which can be considered OK.

Web site: www.quickheal.com
Minimum System Requirements: Windows 9x/ME/NT/2000/2003/XP, Pentium 133 MHz, 32 MB RAM, 40 MB hard drive space

3.2.3.5 Trend Micro PC-cillin Internet Security 2006

Trend Micro's PC-cillin Internet Security 2006 is a comprehensive internet security suite which includes anti-virus, anti-spyware, and anti-spam protection, as well as a personal firewall, private data protection, and Web-content filtering. It has an easy-to-use yet powerful interface.

There is an "Antifraud" feature, which protects you against fraudulent messages, Web sites, and other forms of phishing attack. AntiFraud includes Antispyware, Spam and Fraud filter, Web Site filter and Privacy Protection.

PC-cillin's easy yet powerful interface

The anti-spyware module can be used to get rid of spyware and it is memory resident, theoretically preventing spyware to get installed in the first place. Its built in firewall also supports WiFi intrusion detection, which we did not see in any other software we tested. It is much easier to have your wireless network hijacked since this does not involve a physical connection. It is possible that such an intruder could access private data on your machine, or perform other malicious activities. If you enable Wi-Fi detection, Internet Security will scan your network at a specified interval, and warn you when new computers connect. Other computers running supported Trend Micro software can be marked as Trusted.

It scans incoming and outgoing e-mails and can scan inside archives received as attachments. Some of the supported e-mail clients are Becky! Internet Mail 2.0, Eudora 6.2, Microsoft Outlook Express 6.0, Microsoft Outlook 2000, 2002, or 2003, Mozilla Thunderbird 1.0, and Netscape 7.2.

The Spam filter processes e-mails and prefixes, "spam:" or "phishing:" to the subject of a suspect message. A toolbar that integrates with Outlook and Outlook Express can be installed. This bar can be used to add a sender to the approved or blocked list, or to report a message to Trend as spam, fraudulent, or not spam.

The firewall allows few programs to automatically connect to the Internet. Moreover, you don't have the option of allowing a program to connect just once. You can either set the program to always access or always deny.

The Privacy Protection and Web Site Filter features were up to the mark. You can add sensitive data in the Privacy Protection screen to be marked as Private. You can choose to prevent such from being transmitted via instant message, e-mail, or a Web form, optionally exempting specific sites such as your online banking Web site. When someone attempts to send such tagged

data, the transmission is blocked, the attempt logged and a notification is displayed.

The AntiFraud toolbar for Internet Explorer shows a site's credibility rating and one of preset Web filter categories defined by Trend Micro such as Phishing, Spyware, Adult, Crime, etc.

During the test scan, we found that the PC-cillin Internet Security 2006 was reasonably easy on system resources. Its scanning time was the lowest at five and a half minutes. The average response time of between 6 and 8 hours means that it is not the fastest of the companies to response to outbreaks.

Web site: www.trendmicro.com
Minimum System Requirements: Windows 98/ME/2000/XP, Pentium 233 MHz, 128 MB RAM, 100 MB of free hard drive space

3.2.3.6 ZoneAlarm Anti-Virus

ZoneAlarm Anti-Virus also comes with a basic firewall. The installation of the program is very simple and the program is updated during this process. At the end of the installation, you can review the security settings and launch ZoneAlarm Antivirus. The interface of the program is very easy to get around. The main or overview screen shows the status of the incoming and outgoing traffic of the firewall and the number of programs that have been allowed access to the internet during a session. You are also provided information about the e-mail scan and on-access, anti-virus scan status.

You need just one click to scan your computer after you launch the Anti-virus from the system tray icon. But if you need to scan a folder, you need five additional clicks to do so. While you can specify which folders to scan, we did not find any options to specify the type of files to scan or whether or not to scan compressed files. So each time you scan, compressed files are also scanned.

It supports a wide variety of protocols for e-mail protection such as HTTP, IMAP4, POP3 and SMTP. A large number of instant

messengers are also supported: MSN, Yahoo!, AOL, AIM, ICQ, Trillion, GAIM and Miranda.

The ZoneAlarm Anti-Virus interface

When we ran the test scan, we found that this anti-virus requires the lowest memory in this category, which was 278 MB or 50.27 per cent. The CPU resources used were higher though at 32.18 per cent. The scanning time was also very slow. It took about 19 minutes to complete the test scan.

The outbreak response time of this company was the slowest, taking between 18 and 20 hours, which leaves the computer vulnerable to viral attacks for quite a long time.

Web site: www.zonelabs.com
Minimum System Requirements: Windows 2000/XP, Pentium III 450 MHz, 64 MB RAM, 50 MB of free hard drive space

3.3 Viruses In Linux

So here's the general perception: Windows is prone to attack and needs tons of patches, while Linux is a stable operating system that suffers from no viruses. One reason commonly given for this by those who love Microsoft is that there aren't so many Linux machines around, and as Linux becomes more popular, there will be more viruses for that platform.

It's something to think about. But even before we tell you that there do exist viruses for Linux, here's a snippet of what Scott Granneman of online computer security news portal SecurityFocus had to say about the issue, in 2003:

"We've all heard it many times when a new Microsoft virus comes out. Someone on a mailing list or discussion forum complains about the latest in a long line of Microsoft email viruses or worms and recommends others consider Mac OS X or Linux as a somewhat safer computing platform. In response, another person says, basically, 'How ridiculous! The only reason Microsoft software is the target of so many viruses is because it is so widely used! Why, if Linux or Mac OS X was as popular as Windows, there would be just as many viruses written for those platforms!'

"Of course, it's not just "regular folks" on mailing lists who share this opinion. Businesspeople have expressed similar attitudes... including ones who work for anti-virus companies. Jack Clarke, European product manager at McAfee, said, 'So we will be seeing more Linux viruses as the OS becomes more common and popular.'

"Mr. Clarke is wrong."

Granneman goes on to explain why, but what he said reinforces the idea that Linux is inherently more secure, and that may be true. But we must also point out that there have been Linux security incidents involving viruses. In addition, there do exist Linux anti-virus tools.

It's a controversial subject. Ask a Linux aficionado and he'll tell you about file permissions and such, and how Linux users don't need to worry at all; ask someone marketing security products, and he'll tell you the urgency of the need to bolster Linux systems.

"Linux will be a target because its use is becoming more widespread," said Raimond Genes, European president for anti-virus at

security firm Trend Micro, echoing Clarke. "It is a stable OS, but it's not a secure OS."

Clarke has also said that it's probably *easier* to write a virus for Linux because the code is available." He has gone on to say that it seems "ridiculous" that users have any doubt about Linux being attacked. "It's not a target at the moment because the market isn't there, but Li0n and Ramen (two of the more famous Linux viruses) have already proved that it's on the menu."

Then there's the whole thing about why virus writers write their viruses in the first place. Genes has this to say: "There is some prejudice amongst the virus writing community. If you write a virus for Windows, your peers clap their hands; write one for Linux and they'll stone you."

Genes has also said that we are likely to see more viruses capable of denial of service attacks and more network-aware viruses that use techniques similar to those of Code Red and Nimda, two rather infamous viruses. Nimda, as an example, can set up open shares on a network.

The experts agree that what the virus writers will be concentrating on now is social engineering, which, of course, doesn't depend on the OS.

Grisoft, makers of the AVG anti-virus software, recently warned that it is "only a matter of time" before Linux becomes widely targeted by virus and other malware writers.

Michael Foreman, a partner at AVG UK, said: "In the past few years we have seen the use of enterprise Linux applications growing steadily, and it is only a matter of time before we can expect to see virus attacks specifically targeted at these users.

3.4 Anti-Virus For Linux

As an indicator of how few viruses there are for Linux, you'll find that there aren't too many Linux anti-virus programs around! Here are some of the more popular ones.

3.4.1 BitDefender Linux Free Edition

www.johannrain-softwareentwicklung.de/e_bitdefender_linux_free.htm

Support for this product has been discontinued, so get it from the site above while it's still offered for download! BitDefender features an on-demand scanner for command line or shell scripts, and manual scans of individual files or entire file systems. The site claims that "new, undiscovered threats can be detected and immediately eliminated from the system," though we can't figure exactly how that works.

3.4.2 F-Prot Antivirus for Linux x86 / BSD x86

Visit **www.f-prot.com/products/corporate_users/unix/** . You'll find a range of F-Prot's products, for mail servers, file servers, and workstations.

3.4.3 Kaspersky Antivirus 5.5

www.kaspersky.com/linux

Kaspersky Lab last year expanding into the American market with the US debut of its anti-virus software for Linux and Unix mail servers, file servers and workstations.

"Linux products are much more prevalent in Europe. But as Linux comes more and more online in the United States, there is a greater need for protection against malicious code," said Randy Drawas, a Kaspersky Lab spokesman.

Kaspersky Anti-Virus version 5.5 is designed to protect e-mail servers, file servers and workstations running on Linux, Free BSD and Open BSD operating systems.

3.4.4 Panda Antivirus

www.pandasoftware.com/download/linux/linux.asp

Panda software, makers of one of the most popular online virus scan services, has an offering for Linux: an anti-virus that scans and disinfects Windows and DOS workstations connected to a Linux server, as well as the Linux server itself. The target files of the antivirus are Word documents, Java Applets, ActiveX controls and compressed files.

Panda Antivirus for Linux is freeware, and Panda Software does not offer technical support for the product.

3.4.5 A Parting Word

There's something on the other side of the fence as well, after all this talk of how Linux systems can indeed get infected. Ray Yeargin of Librenix.com has this to say:

"Since there are so few Linux viruses in the wild, who knows if the products actually work? At best, the Linux antivirus hawkers are jumping the gun—trying to capture a market that isn't quite there yet. At worst, they're advancing a cynical ploy to separate Linux newbies from their cash for something they couldn't possibly need."

Food for thought!

Adware And Spyware

What if you bought a music CD and every five minutes a voice came on and asked you to get a new credit card, or to change your mobile service provider, or to have illicit sex with a desperate housewife? And if your music listening habits were constantly being monitored? And if the force behind the voice caused your CD player to eventually go kaput? Translate that to the world that is the Internet, and what you have is adware and spyware.

4.1 What are they?

Essentially, "adware" is an abbreviation for advertising-supported software. Adware comes bundled with some commercial software which, upon installation, installs packages that download advertising material to your computer and display them. These ads are usually displayed when the user is using the original software application. However, this is not always the case. As it becomes increasingly pervasive on your computer, adware begins to pop up ads even when you aren't using the original software application. And that's when it gets really irritating.

An example of common internet adware

Spyware, on the other hand, is irritating right from the beginning. It gets its name from the fact that it installs itself and performs (often malicious) operations on the user's computer without his knowledge. It is intentionally designed to stealthily install itself and monitor the user's activity, accessing information that can easily be used to someone's profit. Essentially, spyware, once on your computer, is used to transmit personal data to a third party that will use it for a purpose you did not sanction.

Spyware shouldn't be confused with viruses or worms, as a spyware package is not intended to replicate itself.

4.2 How Do They Attack?

Adware, spyware, and for that matter, any malware, can attack in a variety of ways.

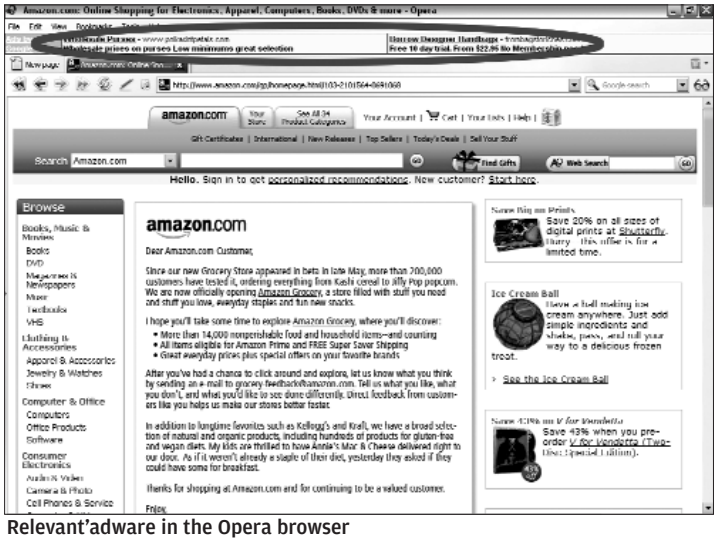
4.2.1 Adware Attacks

As mentioned earlier, adware is usually bundled with a commercial software. It can install itself on your computer either with your permission or without your knowledge when you install the software package. Milder forms of adware are also present in the form of pop-up (and the increasingly common, pop-under) banners that pop up when you visit certain sites. These ads, sometimes referred to as "Java traps," open up in several mini-windows—each time a window is closed by the user, code that spawns another window is activated.

Programmers sometimes add adware to their software packages in order to recover some of the cost of developing the package. If the package is freeware (see box *Some Terms Explained*), then the adware is used to make up for the entire cost of development. Shareware packages also sometimes carry adware that is activated once the trial period is over.

Adware can have several negative effects on your computer. It generally slows it down since it gobbles up some of your system's RAM. It also, to a large extent, slows down your Internet connection, as a lot of bandwidth can be used to download ad content.

Adware is generally licensed content, and therefore usually (though not always) requires the user's permission before being installed on the user's computer. It collects information about how one is using one's computer and the content transmitted



Relevant'adware in the Opera browser

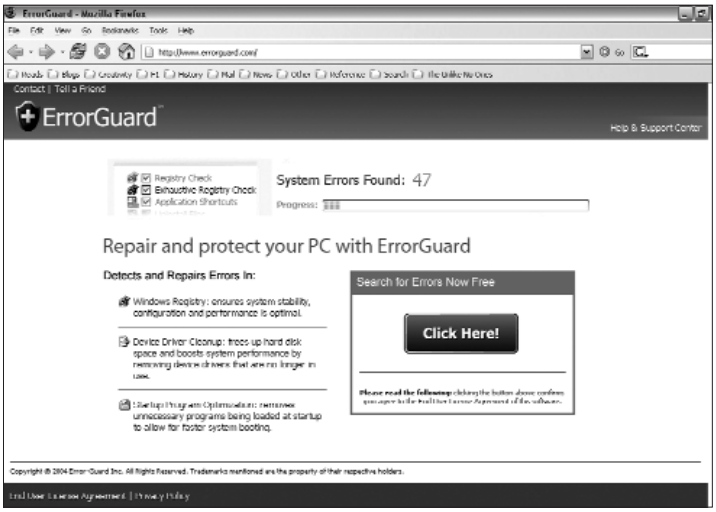
therein, and based on this, displays "relevant" ads in your browser (see screenshot). The free versions of certain browsers, like Opera, used to support adware. Come P2P clients, such as KaZaA, have adware (for example, Gator, TopSearch, etc.) that install on your computer.

However, there are very few examples of such "good" adware. Good adware allows you to uninstall it whenever you like. The other type of adware installs itself on your computer without your permission. Usually, sites with explicit content install such packages onto your computer. These could eventually "hijack" your browser, causing your screen to get filled with more and more pop-ups.

4.2.2 Spyware Attacks

Spyware is intended to gather information about a computer user without that user's permission and knowledge. There are different levels of information that spyware intends to collect from one's computer. The milder versions collect data about the

user's Internet usage and sends it to, say, an online advertising agency, who will then point your browser towards advertising content (read tons of pop-ups). The harsher versions of spyware can take more personal information from your Internet history such as credit card numbers and passwords.



Errorguard is a commonly known application that installs various spyware on your computer

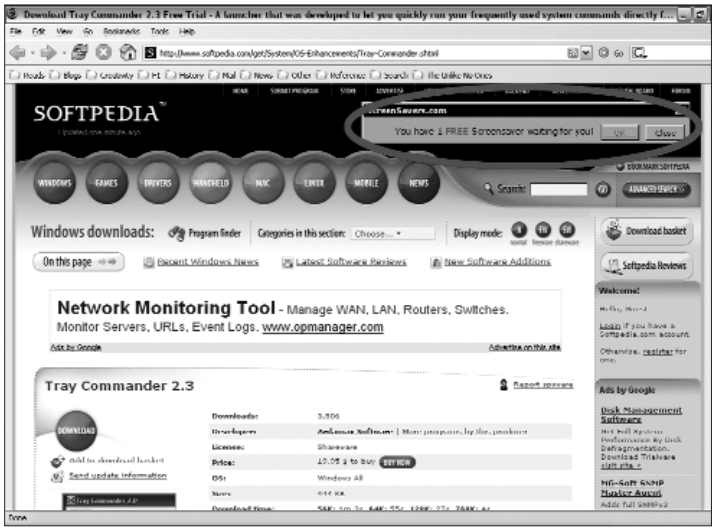
Spyware is usually developed by individuals who want to infiltrate computers and use it to their profit. Spyware, once installed on your computer, can drastically slow down its performance, since it consumes a large amount of RAM; with every subsequent browser function, it slows down your computer further.

But how *does* spyware get installed on your computer? Well, you don't have to visit a pornography site to be attacked by spyware. These days, spyware has pervaded to sites with not only explicit content, but also to sites with other accessible Web content, including downloads from sources that aren't legitimate. Though it may seem pretty cool to have been able to get some

really expensive pirated software off a warez site, you are almost certainly going to be open to spyware as you do it. The same goes for some P2P clients (like Kazaa, BearShare, and Morpheus).

Gator

One of the most common spyware on the Web is Claria Corporation's (formerly Gator Corporation) Gator. Usually, Gator installs itself with such applications as DivX Pro or KaZaA. However, Gator can also install itself even if you haven't installed these programs. Most malicious Internet advertising will guide you to some or the other "free" software download. And if you do download such software, nine times out of ten, Gator will be installed on your computer without your knowledge.



Links like this usually lead to a Gator installation

Spyware can get installed on your computer when you install certain software, through the ActiveX controls of malicious Web sites, or even through pop-up advertising. ActiveX is a technology used by Microsoft IE, and it allows different applications—or parts of them—that you installed on your computer to be accessed by your browser to display content. Some spyware developers are particularly cunning, disguising their spyware

programs as spyware removal programs, thereby fooling users into downloading more spyware.

Spyware programs are getting more malicious by the day. They could install a variety of application DLLs on your computer that allow hackers to snoop on what you're doing. These DLLs can do a variety of things to your computer—monitor your keystrokes

Some Terms Explained

Freeware
As the name suggests, freeware is software that is available for download and use free of charge. The essential difference between freeware and adware is that freeware is free software without advertising content. Freeware also does not usually come with technical support on the developer's behalf. As opposed to shareware, freeware can be used indefinitely and does not expire after a particular period of use.

Shareware
Put simply, shareware is "try before you buy" software. Shareware allows you to use the software for a trial period, after which you are asked to purchase it. The purchase may be of the entire software package, or a registration code to unlock the original shareware package for unrestricted use. The best part about shareware packages are that they allow you to evaluate them before actually buying, so you know whether the package suits your requirements or not. And as the name implies, users are encouraged to *share* the shareware package with friends.

Warez
Warez is essentially pirated stuff (games, applications, music albums, *et al*) that are available for download over the Internet. There are clear violations of copyright laws in downloading and using warez.

on or offline, access your word processor, hijack your Web browser, display advertisements, and more. And some spyware leaves your computer even more open to attack from other spyware.

Gator basically displays advertising on the computer on which it is installed. It also installs a host of other applications like GotSmiley, Dashbar, and more, which further slow down your computer.

4.3 Installing Freeware Wisely

Though one cannot be 100 per cent safe, there are some simple rules one can follow while installing freeware, or 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 legitimacy or the trustworthiness of a download source, it would be advisable to look elsewhere.

❍ Though it can be a pain, it is definitely worth the while to read the Terms of Agreement of the software. 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. The golden rule is: only install software the contents of which you're sure of.

❍ Spam is one of the leading sources of spyware. A large amount of spyware (posing as Trojans) is spread through e-mail.

❍ Use your discretion and a general sense of caution when clicking on Internet ads (if you do). A lot of banner ads have buttons that say "Cancel" or "No" that you're prompted to click if you don't want the product they offer. Do ~not~ click that button! More often than not, doing that will take you to another ad site. If you are unsure about what to do, just close your browser window.

❍ Everyone needs pop-up blockers, and luckily, most new versions of popular browsers have pop-up blockers already inbuilt. It is advisable to install the latest version of your Web browser.

4.4 Removing Adware And Spyware

If you've been regularly downloading and installing freeware or shareware applications, chances are your computer is infected. The same goes for clicking on pop-up ads or banners, or using P2P clients.

Trend Micro offers a free online spyware scanner

There are several trustworthy services that can scan your computer online. Trend Micro's House Call (**www.trendmicro.com/hc_intro/default.asp**) is one such offering. It scans your computer for not only spyware and adware but viruses as well.

Identifying spyware and adware is the easy part; getting it off your computer is the tough bit. Spyware is intended to be difficult to find and not very easy to remove. Most spyware are hidden in a variety of directories on your computer—removing them is really not as easy as using your Add/Remove Programs applet. It is made tougher still by the fact that some of these applications come bundled with freeware and shareware applications, and removing the adware can disable the functionality

of the original application. However, there are several applications that can make your life easier.

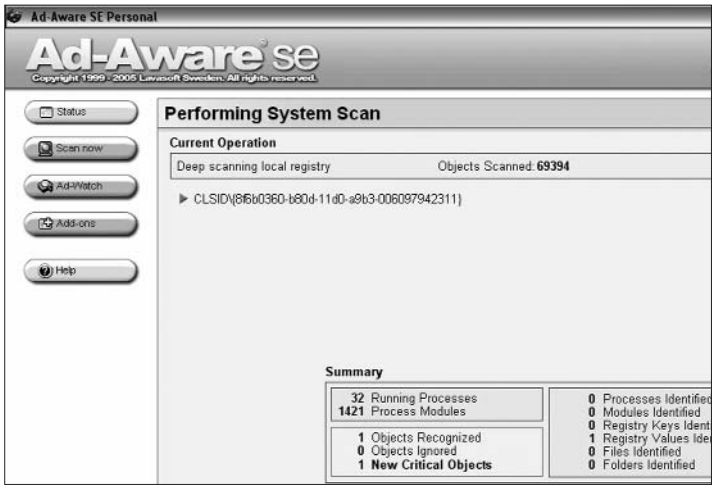
4.4.1 Ad-Aware

http://www.lavasoftusa.com/software/adaware

By far the most popular adware and spyware removal tool is Ad-Aware from Lavasoft. There is a freeware version available for download at the Lavasoft Web site. The software features powerful search and removal tools that help detect and eliminate spyware from your computer efficiently and effectively.

The advantage of Ad-Aware for a personal home computer user is that it performs a quick scan that is effective enough for removal of not only spyware and adware but also Trojans, keyloggers, and more.

Ad-Aware can detect spyware programs running in your system's memory, examine your system's startup settings, deal with browser hijacking, remove tracking cookies (which track the sites and information you access on your browser), and fix



Ad-Aware performs a pretty deep system scan

any changes to the Registry that have been made by spyware and adware programs. The best part about Ad-Aware is that it can get rid of stubborn spyware.

The application, however, does not have some key functions. For example, it does not let you schedule spyware scans. You can only configure it to run scans at startup, or manually when you choose. Also, its real-time scanning (similar to an anti-virus that detects when a virus is attempting to attack your computer) is not as efficient as that of some other programs. Still, the program makes up for this with its easy-to-use interface and customisable scan options. You can choose the level of thoroughness you want to run the scan at, from a deep system and archive scan to a simple surface scan.

The program also downloads spyware and adware definition updates to keep your computer on track all the time.

Spybot has very powerful spyware detecting functionality

4.4.2 Spybot Search and Destroy

www.spybot.info/en

Ad-Aware may be the most popular spyware scan and removal application, but Spybot Search amd Destroy is considered by many as the better option. The interface is not as slick as that of Ad-Aware, but it is a much more feature-packed application with a variety of components that Ad-Aware does not have, like the Scheduler. It is also a much more detailed scanner.

Right from the start, you know the program means business. It informs you that if you remove spybots (Spybot's term for spyware applications) from your computer, you may not be able to use the host programs that the spybots were bundled with.

Spybot's interface is very functional; there's a toolbar on the left, and details on the main screen at the right. You can choose to view the Default mode or the Advanced mode. The Advanced mode offers several extra options such as IE tweaks, Secure Shredder, etc.

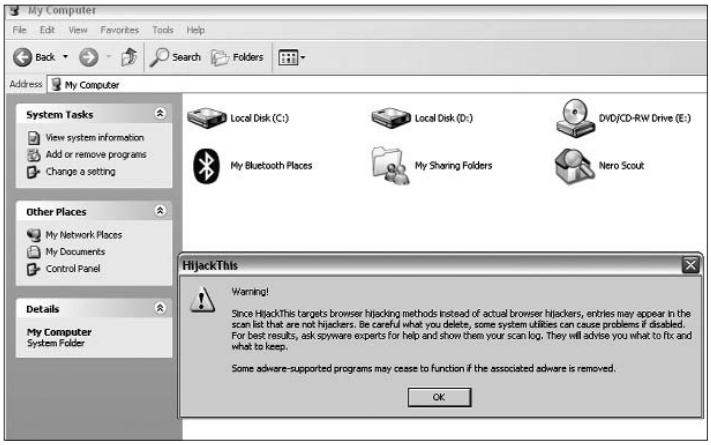
After scanning your system, Spybot lists out the harmful entries on your computer so you have an idea of what exactly is going on. You can check the entries you wish to delete, and if you're unsure about what to do, the software will give you a few options and a detailed explanation of what the entry is, along with a recommendation. One feature is that if you decide to keep the adware on your computer, you have the option of excluding it from further scans. You can also instruct the software to exclude a host of other components that you may feel like keeping on your computer, such as cookies.

Spybot, like we mentioned, has a lot of functions that are absent in Ad-Aware, such as the "exclude" functionality. One of the best options Spybot offers is in the Immunize menu. This allows you "immunise" your browsers to malicious content, so that a spyware program, once removed, is not allowed to enter your computer again later.

4.4.3 HijackThis

www.merijn.org

Before we discuss what HijackThis is and what it does, we need to have an idea of what essentially a browser hijack is. A browser hijacker, as the name suggests, is a form of malware that "hijacks" your Web browser and displays tons of pop-up ads one after the other. It replaces the existing start page, search page or error page of your browser with ones of its own. This results in



HijackThis gives you its statement of purpose

the opening of your browser—and subsequently your computer—to harsher spyware attacks.

So, essentially, what HijackThis does is lists all the installed browser add-ons, start-up settings and buttons that may have been installed on your browser with or without your permission. HijackThis scans special zones of your Registry and hard drives, and lists the contents of these areas—those that are generally accessed by browser hijackers. It is up to you to decide what to delete and what to keep. However, the software does give a description of what the entries mean, and makes recommendations.

The application executable is just 213 KB, and gives you the option of a plaintext log file of the entries found on your Registry and hard drives. Most of these entries can be removed or disabled by the software.

You should, though, be sure of what you're deleting or disabling, as you may inadvertently disable a key function of your computer. And this is where HijackThis lacks. It is not meant for novices. A little knowledge of your system Registry is a must.

Beginners are advised to use software with more user-friendly interfaces like those mentioned above, though they don't provide such powerful browser hijacker deletion features.

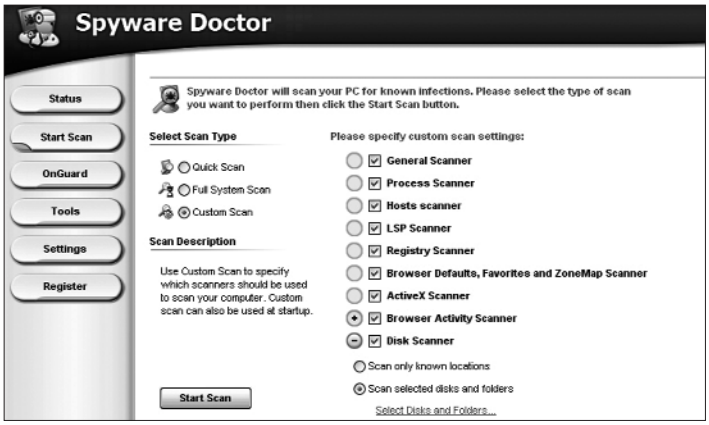
It is recommended that you unzip (you don't need to install the software—just download the .exe file) HijackThis to a known directory rather than a temporary directory, as you will not be able to undo any errors that have been corrected by HijackThis from a temporary directory—the default location that the software unzips into.

4.4.4 Spyware Doctor

www.pctools.com/spyware-doctor

Spyware Doctor is an efficient spyware removal tool from PC Tools. It performs a pretty deep system scan for almost all current spyware, and the best part is, it sits in your system tray, monitoring spyware activity on your computer. The system scanner is highly customisable, and you can define the system areas you want to exclude from the search.

The interface is attractive and user-friendly. However, the software is subscription-based, and once the trial period is over,



Select what you want to scan with Spyware Doctor

you are asked to purchase a registration code, or you will not be able to retrieve updates.

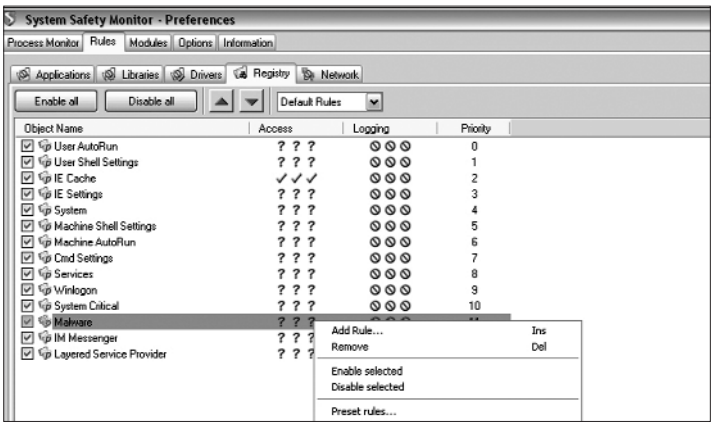
The best feature of Spyware Doctor (and also the one you are eventually asked to pay for) is the OnGuard feature. This is the tray monitoring functionality of the software. It keeps itself up to date with the latest spyware definitions with its very regular Live Update feature.

The software also lets you undo any changes you made when disabling or removing spyware, so that you do not inadvertently lose the host program's functionality in the process. Spyware Doctor features one of the fastest full-system scans.

4.4.5 System Safety Monitor

www.syssafety.com

SSM has a broader mission statement, so to speak, among spyware removers. It is intended to stop any malicious software from operating on your computer, and basically to block such applications from installing themselves on your computer. As its name suggests, it is essentially a monitor, so it works more like a real-time anti-virus than as a scanner/remover.



Choose the types of Rules you want SSM to set

What the program does is set "Rules" for the processes running on your computer, and alert you if changes are made to these, or if any new processes are attempting to be opened. This way, if any malicious application is trying to enter or start on your computer, you will be shown an alert (from the system tray) and will be prompted for the action to be taken—whether to allow it or block it.

SSM may seem a little annoying at first, since when you open any application on your computer, be it your browser or your word processor, it will prompt you for an action. However, you can disable whatever rules you like.

The software is not very novice-friendly, and it takes a little time to get a hang of all the functionality it offers. Also, the latest version, 2.2.0.581, offers only a 30-day trial, after which you are asked to buy a registration key.

4.4.6 Microsoft Windows Defender Beta 2

www.microsoft.com/athome/security/spyware/software/default.mspx

Microsoft released their very first free antispyware product—Windows Antispyware in December 2004. This was later renamed to Windows Defender and is now available as such. To download this, you need to use a genuine copy of Windows because this download comes under the Genuine Windows Advantage downloads from Microsoft in which your copy of Windows is verified online for its legality.

During the installation, you are asked whether you'd like to use the system's default settings for SpyNet participation (see below) or choose other options. Being a Microsoft product, we were hardly surprised to note that its interface blended well with Windows XP's. A toolbar at the top is used as the primary interface with Forward and Back buttons and buttons for Home, Scan, History, and so on.

The Home screen provides you information about the state of your computer: whether your spyware definitions need updating, the last time you scanned your system for spyware. Clicking on the Scan button will initiate a quick scan of your computer. If you wish to do a selective scan, you can do so via the drop-down arrow adjacent to the Scan button, which allows you to start a Custom Scan. Clicking on the Tools button lets you set a variety of options such as 'Allowed items', where you may exclude certain applications that are known to trigger false alarms. The last option which is Software Explorer lets you view processes in your Windows, but with much more information than the Task Manager offers, such as the name of the process and what else is running within that process.

Windows Defender is memory resident. Surprisingly, there is no system tray icon for this application. Archive formats such as ZIP are silently scanned and stopped before a spyware can be installed. It works in conjunction with IE 6 and 7 in Windows XP SP2 and 2003 SP1. It can block attempts to run suspect files. Automatic update keeps the Windows Defender up to speed by downloading the latest spyware definitions from Microsoft's Web site.

4.4.7 SpywareBlaster 3.5.1

www.javacoolsoftware.com

SpywareBlaster from Javacool Software is a free antispyware with a difference. Unlike similar applications, this one does not run in the background all the time. The installation is fairly simple and on the first run, you are guided through an introductory tutorial.

The main screen displays security information on your system and possible steps needed to increase its security.

The SnapShot section lets you take a snap of your system while it is in a good, clean state and save it or restore to it, similar to the System Restore option in Windows XP. The Tools

section lets you configure options such as Hosts Safe which stores a backup copy of the Hosts file so that it can be restored later. It also has something called Flash Killer which completely disables downloading of Flash content which, more often than not, are advertisements. A Custom Blocking option lets you specify ActiveX controls which you may wish to block. Then there is the Update option to update this software.

When we minimized the application, SpywareBlaster informed us that it is not necessary to run it in the background. As we found out, it does not actually scan your computer for spyware, it addresses the root of the problem by not allowing spyware to be installed in the first place. As you may have seen, it blocks paths of installation of spyware which are ActiveX content, browser hijacking applications, Flash content, etc. It disables the CLSIDs of popular spyware ActiveX controls, and also prevents the installation of any of them via a webpage. This allows you to run Internet Explorer with Active-X enabled, but it will never download or even prompt you for any of the known ActiveX controls. All other Active-X controls or plug-ins will work fine.

Data Security

Securing your data goes beyond paranoia—it is often vital, although paranoia does drive much of data security. Physical files and folders can be locked away without your having to give much thought to it, and in this chapter, we look at the virtual equivalent of that

5.1 Encrypting Your Data

5.1.1 Using Windows XP Pro

The most obvious way of locking away your data is to encrypt it, and this can be done at various levels: encrypting individual files, or folders, or entire drives. Windows XP Professional offers an easy way to encrypt files and folders. Just follow the steps below to ensure no-one who has access to your computer can open certain files or folders. Note that this method doesn't use passwords—the way it works is, when you're logged on, the contents of the file are visible; when someone else logs on as a Guest or under a different login, he won't be able to see the contents of the encrypted files or folders.

To encrypt a file or folder, right-click on it and select Properties. In the General tab, click Advanced. Check the "Encrypt contents to secure data" box.

If you chose to encrypt a single file, you can also choose to encrypt the containing folder. Select "Encrypt the file and the parent folder" in the Encryption Warning dialog window. All files created in the encrypted folder will be automatically encrypted then on.

To decrypt the file or folder you encrypted—which you don't need to do if you're the only person who logs on to your machine—just do the following: right-click on the file or folder, click Properties, and in the General tab, click Advanced. Then clear the "Encrypt contents to secure data" checkbox.

When you decrypt a folder, you need to decide whether to decrypt only the folder or to decrypt the folder and all files and sub-folders in the folder. If you choose to decrypt only the folder, the files and subfolders within the folder will remain encrypted. But when you add new files and sub-folders to the folder, they will not be automatically encrypted.

5.1.2 Simple Context-Menu Encryption

There are many, many freeware utilities out there that offer simple, one-click encryption. You right-click a file, select "Encrypt", supply a password, and that's it—the file won't open again until the correct password is supplied! One example we came across is Crypt4Free, at **www.secureaction.com/encryption_free/**. This isn't a software we're particularly recommending, but it's a good example of all the software out there that can do this for you and make life a little simpler. Wrote a mail you don't want anyone to see? Encrypt it! Took down some notes at office in a text file that no-one else should be looking at? One right-click and a password later, and you're done! It really is that simple.

Alas, such software are a dime a dozen, and where they lack is in the following areas:

❍ If you forget your password, you have no way of recovering your file. No password hints!

❍ The same holds even if you mistype your password. You'll have no way of knowing that you mistyped it, and the file will get encrypted—gone for good.

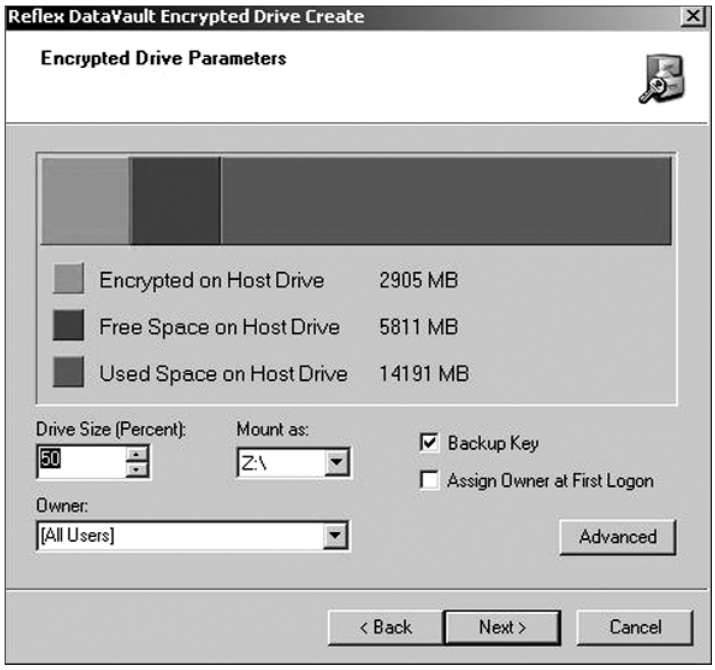
❍ Such software typically cannot deal with large files, and give errors when you try to do it—or they hang your computer.

❍ There's no way of managing all the files you encrypted, from one central location.

❍ These usually don't come with support for folder encryption.

5.1.3 Comprehensive Encryption Software

If you're willing to go paid, you'll get software that encrypts entire drives for you, creating virtual folders where you can store anything you want to in encrypted form. An example is to be found at **www.reflex-magnetics.co.uk/products/datavault/**



Reflex DataVault offers rather advanced encryption features

page5 . "Reflex DataVault" appears as a standard hard disk in My Computer, and standard Windows Explorer operations can be used to access and save data within the encrypted drive.

Again, we're not making a recommendation: this example is only for illustrative purposes. What you get at the site mentioned above is a software that offers, amongst other things:

- Virtual hard disk encryption
- Simple save it / encrypt it functionality
- Securing of sensitive data while on the internet

- Supports multiple user access
- Provides secure data transfer when changing notebooks
- Secure challenge-response password recovery

This pretty much takes care of all the drawbacks we mentioned for the "encrypt with one right-click" type of software we described earlier.

Such functionality doesn't come free, of course: Reflex DataVault will set you back by £55 (Rs 4,800). Could be worth it if you're the paranoid type, or if you're the executive type who seriously can't afford someone taking a sneak-peek into your stuff.

5.2 Keeping Passwords Safe

Some of us just remember our passwords, even if they're as ridiculously uncrackable as "gb65end0x", and even if there are many of them to remember. Some of us are naïve enough to use passwords like "azsxdc", and have trouble remembering even those! If you fall in the second category, forget it—someone's going to steal your data soon enough. No, seriously, what one needs is good, strong passwords, and password management software to keep them safe.

A "strong" password is one that has a sufficient number of characters—some say anything over eight will do—and a mix of lower-case, upper-case, and special characters. On top of that, there's the issue of multiple passwords: if you set the same password for everything, there could be a problem. What if your Windows XP and your Gmail password are the same, and a friend of yours wants to access your machine? And then what if you gave him the password to your machine, and he went ahead and tried it on your Gmail account as well? Multiple passwords are, therefore, important. And it's tough to remem-

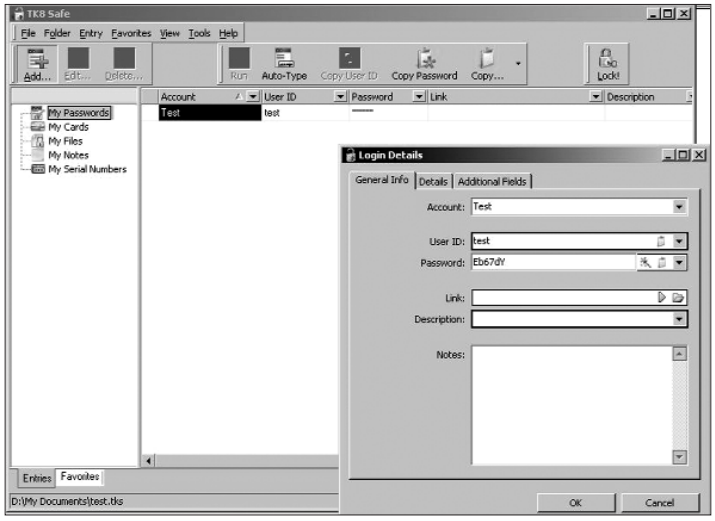
ber multiple strong passwords—and that's where password management software come in, like we said.

These are, again, a dime a dozen, but they're not all bad. Again, we're making no recommendations, and are just providing an example: for $19.95 (Rs 900), you can purchase TK8 Safe, a relatively simple software, from www.tk8.com/safe.asp .

With TK8, you can keep all usernames, passwords, secret notes and serial numbers in one secured database file. The file is, naturally, encrypted.

You can use folders in your files to group information. In addition, you can log in to password-protected Web pages automatically. The password file can be locked, and even if you forget to lock the file, the program does this automatically after it's unused for some time.

Advanced options include multi-user support, additional



TK8 is very powerful, yet easy to use

encryption methods, and automatic password backups. You can run the program directly from removable media like USB sticks. This means you can literally carry all your passwords in your pocket.

Now, we didn't intend this to be an ad for TK8; our intention here is to tell you all that a password manager can do for you. More advanced software simply have more frills.

5.3 Metadata In Documents

Metadata—information contained in a document about the document itself—is present in all MS Office documents. It includes document properties and document history. It can also include things you deleted from the document, but which are still contained unseen in the document when you, for example, sent it across to someone! Naturally, from a security standpoint, you wouldn't want to share metadata, in most cases: you send across that which is final, and there's no reason for the other person to know what you did with the document before you finalised it.

In Word documents—and, in fact, in all Office files—metadata is stored in the Properties and Custom Properties of the document. These are stored internally within the document file in a special format called "OLE structured storage."

5.3.1 Get Paranoid!

As an example, most Word document contain a revision log, a listing of the last 10 edits of a document, showing the names of the people who worked with the document and the names of the files that the document went under. Revision logs are hidden and cannot be viewed in Microsoft Word itself—you need a metadata viewer to do that. In many cases, you wouldn't want to divulge this information.

Here's something that could terrify the paranoiacs: in 2003, the British government published a dossier on Iraq's security and intelligence organisations, which was cited by Colin Powell in his address to the UN the same month. Dr Glen Rangwala, a lecturer, discovered that much of the material in the dossier had been plagiarised from a US researcher on Iraq.

The following is some of what appeared in the metadata for that file, which the British government published as an MS Word document on their Web site:

Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1 \Temp\AutoRecovery save of Iraq—security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\ Temp\AutoRecovery save of Iraq—security.asd"
Rev. #5: "JPratt" edited file "A:\Iraq—security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq—security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq—security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\ Desktop\Iraq.doc"

Notice the names? P Hamill, J Pratt, A Blackshaw, M Khan! Of course, your documents probably aren't as sensitive as those published by the British government, but they could be sensitive nevertheless.

5.3.2 Metadata In Word

Taking Word as an example, the metadata contained in a document includes your name and initials, your organisation name, the name of your computer, the name of the network server or hard disk where you saved the document, the names of previous document authors document revisions and versions, template information, hidden text, and comments!

Open Word. Then go to **File > Open**. In the "Files of type" list, click "Recover Text from Any File", locate a Word file, and click Open. The document will open without any formatting. Look at the information at the end of the document—you may see stuff such as the name of the author and path of the document.

Microsoft themselves say that before you provide others with a copy of your document, it's a good idea to view any hidden information and decide whether it's appropriate to store that information. We're wondering why there isn't an option that says "Store no metadata"!

5.3.3 What To Do

The following are some steps you can take if you want to avoid sending metadata.

❍ Go to **Tools > Options**, then click the Security tab. Select the "Remove personal information from this file on save" checkbox in the Privacy options area, and click OK. Then save the document.

❍ You can also manually remove information from an already-stored document. Go to **File > Properties**. The Summary, Statistics, Contents, and Custom tabs may each contain information that you will want to remove. To remove it, highlight the information in each box and press [**Del**].

❍ Trying to remember the above for each of your documents, or ensuring that the others in your company do this, isn't always practical. Fortunately, Word also provides the RemovePersonalInformation property, which, when set to True, removes all user information from comments, revisions, and the Properties dialog box when the user saves a document.

The following procedure creates a new document and adds code to the document's Open "event" that sets RemovePersonalInformation to True. This ensures that person-

al information will be removed from the document whenever the user saves it. For the procedure to take effect, you must close and then re-open the document. Follow these steps:

Create a new blank document. Go to **Tools > Macro** and click Visual Basic Editor. In the Project Explorer window, under the folder for the current document, double-click "ThisDocument" under the "Microsoft Word Objects" folder. Then in the Code window, click the arrow beside the Object drop-down list, and click Document. Click the arrow beside the Procedure drop-down list, and click Open. Insert the following between **"Sub Document_Open()"** and **"End Sub"**:

```
ThisDocument.RemovePersonalInformation = True
```

Close the Visual Basic Editor by clicking Close and Return to Microsoft Word on the File menu. Save and close the document. When you re-open the document, the document's Open event will execute. Personal information will then be removed from the document whenever the user saves it.

❍ Word can save one or more versions of your document in the same file. Those versions are saved as hidden information. Because these hidden versions are available to others and because they do not remain hidden if the document is saved in another format, you may want to remove these versions before you share the document. Here's how to delete the unwanted versions and then distribute the document: Go to **File > Versions**. Click the version of the document you want to delete. To select more than one version, press and hold **[Ctrl]** as you click each version, and then click Delete.

5.3.4 Going Paid

If you're sceptical of what you can do all by yourself, or if you want to be more thorough—or if you just plain want the peace of mind that a piece of software is doing the work for you, you'll have to be willing to spend. You might also want to go the

third-party way if you're managing a business and are worried (by now!) about metadata in documents.

Here's one site to take a look at: **www.payneconsulting.com/products/metadataretail**. Note that this is not a recommendation on *Digit's* part, but only an example of what's available.

Available at that site is The Metadata Assistant, which analyses Office files to determine the type and amount of metadata that exists. The software allows you to analyse and clean files of metadata. The Metadata Assistant can also be used to batch-process multiple files on a local or network folder. Additionally, you can analyse and clean files attached to mail messages and convert them to the PDF format for extra protection.

Metadata Assistant costs $79 (Rs 3,500).

5.4 Miscellaneous Security Measures

5.4.1 Macros and Macro Viruses

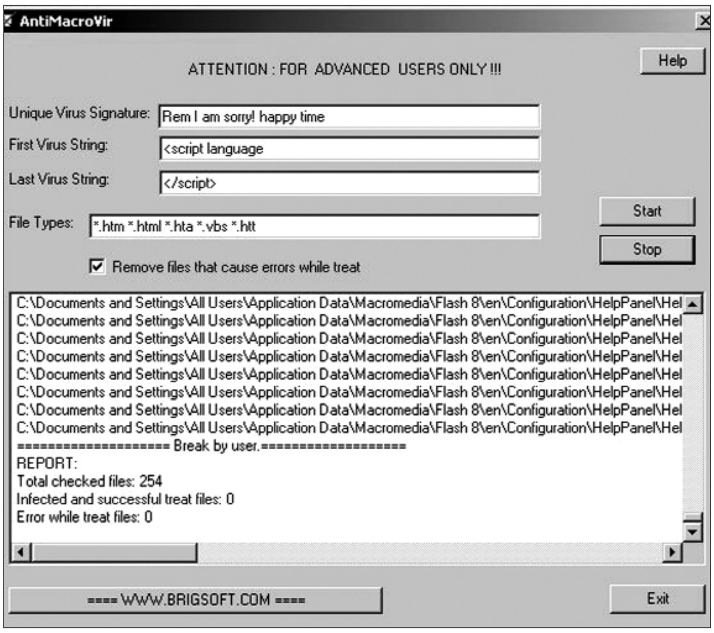
Macro viruses are viruses that infect documents—files created in different applications which do not contain not only data (texts, spreadsheets), but also macros, which are programs created in a special high-level language. Such viruses can spread from one document or computer to another.

In a little more detail, a macro is a sequence of keystrokes or commands that are used to automate repetitive tasks. Today's macro languages are very powerful and can be used to write a virus that can be just as dangerous as other types of viruses. Since they work in Word they can be worse than other kinds of viruses by doing nasty things like putting passwords on documents or adding offensive messages to printouts. Any menu item in Word could be a trigger for the destructive payload.

Word has some special Macro names that are run at certain times. For example, a macro virus in AutoOpen would be run when you open a document and would can copy itself when you open another document. There are many other ways a macro virus can spread from one document to another.

Since the virus is in NORMAL.DOT, reinstalling Word won't remove it. Deleting the NORMAL.DOT file won't remove the virus either because it will just become reinfected when one of the infected documents is opened. Also, not all macro viruses infect NORMAL.DOT.

Most of today's Word macro viruses use a temporary file to copy their code to other documents. This temporary file is usually in C:\ and has a SYS extension, but it is not really a system



AntiMacroVir ably complements your regular anti-virus

file. You should delete the file that is detected, but you'll still have to remove the macro virus that created this file.

Almost all Windows anti-viruses have been updated to handle macro viruses, but here's a program we found on the Internet that specifically handles macro viruses. It's called AntiMacroVir, and is available at **www.softpile.com/Utilities/AntiVirus/Review_11182_index.html**.

You'll find several other such utilities on the Internet.

5.4.2 PDF Creation / Protection Tools

PDF is a great way to distribute your documents, not least because of the security options you can insert into them. As a matter of fact, whatever file type you want to secure—for example, an image file—you can convert to PDF and then distribute it, safe in the knowledge that it won't be used in a manner other than what you intended.

There are two things to be mentioned here: one is the creation of secure PDFs, and the other is the protection of those documents. When it comes to the creation of secure PDFs, there are two possibilities—you either have Adobe Acrobat, or you don't.

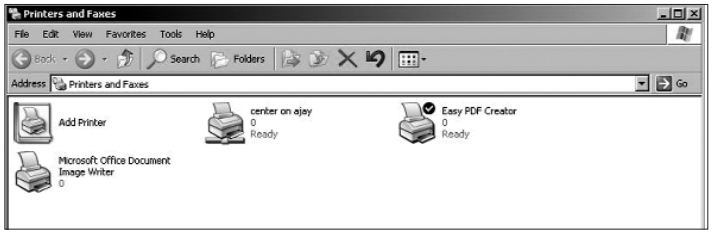
If you do have Adobe Acrobat, after creating your document, just take a look at the comprehensive help file to figure how to secure the document. It's simple—mostly involving using a menu and dialog boxes to specify what activities you want to allow on the document. For example, you can specify that a certain document may not be printed, or that it may not be modified (the most common requirement). To unlock these functionalities, you can assign passwords, and when you want to allow someone to, for example, edit the document, you can convey the password to that individual.

If you don't have Adobe Acrobat and don't wish to pay too much for PDF creation software, there are several applications available. For example, for just $19.95 (Rs 900), you can

download the Pdf995 suite, available at **www.pdf995.com**. Amongst the features offered by Pdf995 are the following:

The Pdf995 Suite offers the following features amongst many more:

- Support for Digital Signatures
- Support for Triple DES encryption
- Integration with Microsoft Word toolbar
- PDF Stationery
- Combining multiple PDFs into a single PDF
- Imposition of Draft/Confidential stamps
- Convert PDF to JPEG, TIFF, BMP, PCX formats
- Convert PDF to HTML and Word DOC conversion
- Convert PDF to text
- Automatic Table of Contents generation
- Standard PDF Encryption (restricted printing, modifying, copying à text and images)
- Support for Optimized PDF and Compressed PDF
- Automatic text summarization of PDF documents
- Configurable Font embedding
- Easy PS to PDF processing
- Specify PDF document properties
- Can be configured to add functionality to Acrobat Distiller



Using Easy PDF Creator is as simple as using a printer

A more professional-looking package can be found at **www.pdfdesk.com/products.html**. Easy PDF Creator costs $139 (Rs 6,300), and that might just be worth it if you can't afford Adobe Acrobat (which retails for $449 (Rs 20,000)). Easy PDF

Creator supports PDF encryption with passwords, and has 48-bit as well as 128-bit support.

If you already have a bunch of PDFs that you need to protect, consider a PDF encrypter. An example (not a recommendation) is available at www.programurl.com/encrypt-decrypt-pdf.htm . The software is called Encrypt & Decrypt PDF, and has a large feature set.

The software allows you to encrypt and decrypt protected Adobe Acrobat PDF files in batch mode. You can secure your PDF files from being printed, changed, copied, extracted, signed, filled, assembled and/or merged, and you also can remove the password from your PDF files, if you already know the owner or user password. All versions of Adobe Acrobat are supported.

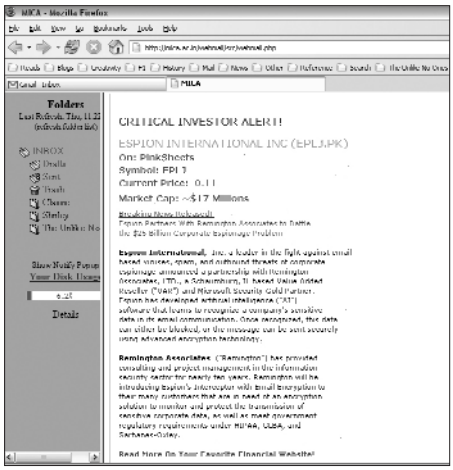
The software supports Adobe Standard 40-bit encryption and Adobe Advanced 128-bit encryption; you can password-protect opening of documents; prevent printing and copying of text and graphics; prevent changes to the document and to form fields and annotations. You can copy and change permissions to an encrypted PDF file.

The Clean Inbox

There was a time when you'd eagerly open your Inbox for those two or three messages you were expecting, and a couple of new ones would actually surprise you. We'd never imagined at that time that we'd one day get 1,569 mails when we clicked "Receive". Read on as we speak about spam in detail.

There is a growing need in the world today to find cleverer, more cost-efficient means of marketing one's brands and products. From putting cars on billboards to hanging men between tall buildings at crowded city locations, they're trying everything today. It was almost inevitable that the online space would become one of the major channels of these messages.

You see them everywhere—banners, pop-ups, the increasingly popular pop-unders, and more. And you aren't left alone to do what you will: the biggest target of these marketing gimmicks has been the innocent e-mail Inbox. From replica watches to products that enhance your sexuality to guns, everything that can be sold *is* being sold... right in the comfort of the Inbox.



If you wanted to buy stocks, you'd go to a broker

Now really, what's the harm if you receive an e-mail or two in your inbox inviting you to sleep with somebody else's wife? Not much, but the scale of operations of spam these days is just too much to even begin thinking about extra-marital affairs. Research shows that the average Inbox receives on an average of between 35 to 40 spam messages every day! And that's an average estimate. In 2004, the California legislature found that spam cost United States businesses more than $10 billion! This included loss of productivity as well as the extra equipment, software and manpower required to combat the problem.

6.1 Some History

Contrary to popular misconception, "spam" is not an abbreviation for "Stupid Pointless Annoying Messages." The term, in the context of e-mail, came from the now-famous Monty Python Spam Sketch. Monty Python's Flying Circus, an early comedy show on the BBC, showed a scene set in a café where every item on the menu had something or the other to do with SPAM meat. (SPAM is a brand of luncheon meat that was rationed to British soldiers in World War II.)

The idea of using this terminology for spam came about when certain users on bulletin boards used to scroll other users' text off the screen by repeating the word "spam" over and over again. They also used several references from the Monty Python scene to achieve their purpose. This sparked off the use of the term "spam" in the way that we know it today.

Spam has grown from being just a means of annoyance to a means of annoying marketing. So now you have, apart from people trying to annoy the hell out of you, people trying to sell you a variety of products you don't really need, at prices you couldn't care less about, using up precious time you really can't afford to spend.

6.2 Phishing

Back to your Inbox: "Get a replica Rolex cheap." "Increase your sexual performance by triple!" "I'm a lonely housewife..." As you scroll through one after the other ridiculous offer, your eye catches something different.

"Before I start, I must first apologise for this unsolicited mail to you... My US client, his wife and children were involved in a ghastly motor accident on such-and-such road in Nigeria ... My reason for contacting you is to repatriate my client's money back to his home country. We need to transfer money into your bank

account..." The mail goes on to explain how there are millions of dollars that this chap needs to transfer to your bank account and how to do this he'll need your account details. You will, of course, be rewarded handsomely for your services.

Identity theft has figured as a criminal activity since time immemorial. Clever thieves have always found that the best way to avoid being caught is to disguise themselves as someone else. And while they are wearing this cloak of disguise, they find it profitable to make use of the identity of the person they are impersonating. No-one needs to be told how valuable one's credit card and bank account details are. But with more and more people using the Internet for online transactions, there is a lot of personal information being shared with a host of companies. Spammers have found an effective way to cash in on this confidence to disclose one's personal information to legitimate sources—phishing.

6.2.1 What's Fishy About Phishing

Phishing is essentially a clever and illegal method used by "phishers" to extract personal information about Internet users. This personal information may be in terms of credit card numbers, bank account details, passwords, and such.

What phishers use is a technique called social engineering. Basically, this means phishers know that people trust the word of someone who *seems* trustworthy. A phisher is thus able to gain the confidence of an individual by posing as someone from a seemingly trustworthy source. Then, the phisher makes the person disclose personal information about himself, and then uses it to his benefit. The Nigerian scam we mentioned above was real: in fact, it was one of the instances in phishing history that led to some landmark legal actions against phishers.

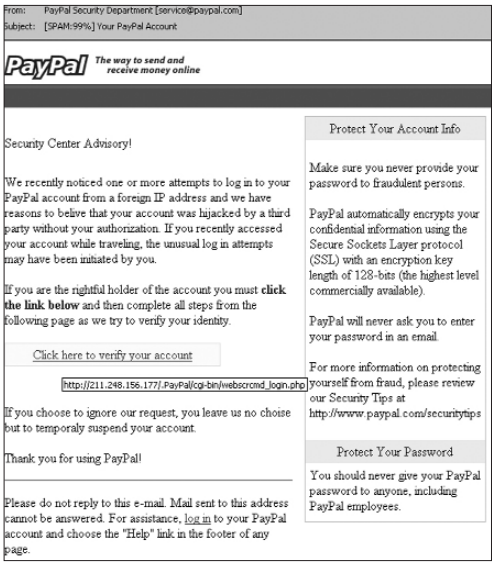
However, phishers don't have to be that straightforward and in-your-face to gain the confidence of unsuspecting individuals. Many phishers pose as administrators of Web sites and request users to send in their passwords. Others pose as bank executives

and ask for your credit card details so you can reactivate your account, or something of that nature.

A good example of phishing in recent times has been the PayPal phishers. PayPal (now under eBay) is an online transaction system. Phishers have posed as PayPal executives and requested people to disclose vital bank information.

6.2.2 How To Tell Something's Phishy

Though the phishers may seem to have gotten their side of the act sorted out, there are some simple ways by which you can detect when there is phishing afoot. Take the PayPal case for example. A phishing e-mail from PayPal does not come with a personal salutation or greeting. Such e-mails are usually addressed to "Dear User" or "Dear Customer".


From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

The PayPal fraud that Phishers commonly use

Phishers' language also suffers from bad grammar and poor vocabulary. You may often find that some e-mails have lots of spelling mistakes, or are written in terrible English. But even a perfectly well-written e-mail is no guarantee of legitimacy. The PayPal phish also had an IP address in the supplied links, which is a giveaway of the legitimacy of the sender.

Phishers commonly use misspelt URLs to trick users into believing that the site that the e-mail will direct you to is the actual site of the company they are posing as. Another telltale sign is the use of the "@" symbol in links: you might find something like "http://www.ebay.in@geocities.com/" . This spoofing method can easily deceive a casual observer who may not pay too much attention to the URLs he is being directed to.

Again, clever phishers will send HTML-based e-mails that look like plain text e-mails, so they can disguise the URL locations effectively. A quick way to fix this is to disable the HTML viewing option in your e-mail client.

6.2.3 But What (And How) Do Phishers Transmit?

Phishers can't be everywhere at all times. So, like good thieves, they get their work done for them. The e-mail medium is the most commonly used, with phishers sending out thousands of malicious e-mails every single hour of every single day. But phishers aren't the only ones sending out such mails. Increasingly, the sources of such mails are becoming home computers that have been compromised by and for phishing activities.

Here's where Trojan Horses (see box *Trojan Horses*) come into the picture. Through various ways (spam, spyware, etc.), phishers install Trojans on unsuspecting home PC users. These computers then become partly (or in some serious cases, wholly) controlled by the phisher who uses the host computer's e-mail client as a mes-

Trojan Horses

A Trojan Horse, or simply a Trojan (the name is derived from Greek mythology) is a malicious program that disguises itself as something interesting, thereby gaining the confidence of the user, who unsuspectingly then installs a piece of malicious software on his computer. Trojans are generally disguised as free screensavers and such, and they arouse the curiosity of those who they are sent to (usually by e-mail). Once installed, the developer of the Trojan is able to gain content from the machine(s) it has been installed on, which can then be used for malicious purposes.

sage propagator. This makes tracking the phish to the original phisher more difficult.

Phishers also transmit a host of malicious content to get valuable private information about individuals. Essentially, these are hacking techniques used by phishers to observe the activities of the users of host computers. This is especially dangerous when the host computer is in a bank, or in a finance firm that deals with large amounts of customer data and large sums of money.

6.2.3.1 Keyloggers

One of the most common spying techniques, a keylogger, as the name suggests, logs the keypresses of the user. Basically, it makes a log of all the keys pressed on the user's keyboard and transmits this log to the phisher.

Actually, keyloggers don't make a log of every single keypress of the user's keyboard: they generally make a log of those keypresses used when the user needs to submit some data for authentication purposes. This could be in terms of passwords, credit card numbers, etc.

6.2.3.2 Screen-grabbing

The more enterprising of phishers capture personal data in the form of screen grabs of the user's desktop. Given that there are already several attempts to block keyloggers by corporations and home users alike, sophisticated phishers find this an effective way of capturing confidential customer/user information. Phishers also don't need a grab of the entire screen for their purposes. In order to keep the upload size of the data small, they only grab the "relevant" sections of the screen wherein there is a disclosure of confidential information.

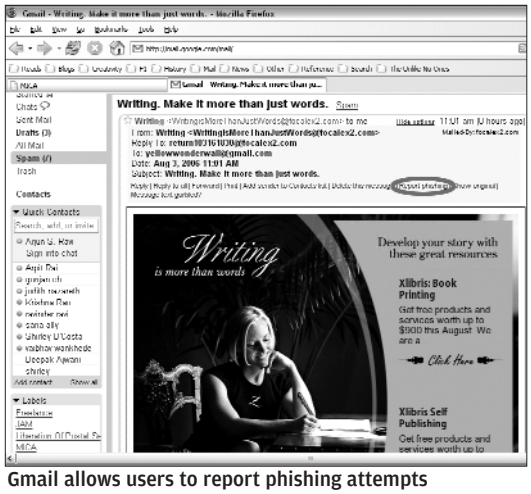
6.3 How Do I Stop The Menace?

A majority of e-mail clients, both for corporate and home use, are now becoming aware of the phishing problem. Most popular free e-mail hosts also offer reasonably decent phishing protection.

E-mail providers are constantly updating their spam filters, which also eliminate phishers. These filters attempt to block phishing attempts in a variety of ways. Apart from scanning for keywords, these filters also attempt to block fraudulent or malicious attachments sent with the e-mail. By disabling the HTML viewing functionality, one can check for the authenticity of e-mails, as phishers usually send malicious mails in the form of HTML mails so as to hide their origin.

Here are simple tips to avoid being phished. Actually, if you're aware of the problem well enough, you're already a difficult phishing target!

1. Phishers usually have a sense of urgency about their e-mails. "To prevent your account from being terminated, please update your details by September 15, 2006." In general, corporations do not like to threaten their customers into action. They'd rather send an annoying sales representative to your house.



Gmail allows users to report phishing attempts

2. E-mails with embedded submission forms are something to avoid like the plague. Never fill out a

form that has been sent in an e-mail unless you are absolutely sure of its authenticity.

3. Sending personal financial information over e-mail is very risky, especially if it has been "requested". If you are submitting financial information on a Web site, look for the "lock" icon in your browser's status bar, which denotes that the source is secure. Some phishers go so far as to create secure Web forms for submitting data, but that's relatively unlikely.

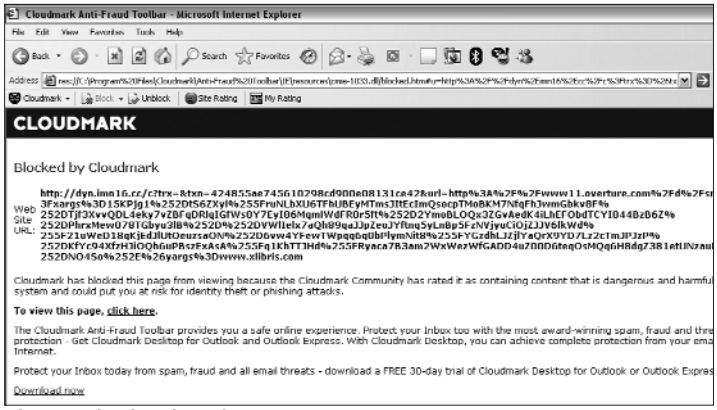
4. View the SSL certificate of the site in question. You can do this by double-clicking on the lock icon.

5. Use a little common sense and judgment when taking a call on e-mails. More often than not, you can tell that an e-mail is suspicious, just by the way in which it is written. A Nigerian prince—especially one who doesn't know you—isn't likely to shower you with money. Don't ask us how some people actually fell for the scam!

6.3.1 Fighting It

Apart from standard spam filters, there are several downloadable tools that can help you block phishing attempts. Phishing generally falls under the purview of spam, so if you are searching for a phishing-only software, you'll probably get a range of anti-spam software that also block phishing.

However, phishing-only tools do exist. One such is the Cloudmark Anti-Fraud Toolbar. The toolbar, meant only for Internet Explorer, blocks you from visiting both phishing sites and sites whose content is not 100 per cent verifiable. The toolbar sits in your browser under the address bar and monitors the contents of the pages you are visiting. It gives you a rating of the site—safe, questionable or unsafe. If the site visited falls in the "unsafe" rating, it is blocked immediately. However, if this is some content that you wish to see, you can unblock the site for viewing.



The way Cloudmark works

Most browsers are becoming quick to the phishing threat. The new Internet Explorer (Microsoft IE 7) browser and the to-be-released Firefox 2 (codenamed Bon Echo) have both installed anti-phishing features. Essentially, both browsers check the URL against a list of known phishing sites, and block or unblock content on that basis.

6.3.2 Pharming

Like phishing, 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 divulge information.

For example, the pharmer could divert your browser from the original Gmail Web site, to a look-alike and then save your username and password. This is a very simple example; there are much further lengths that pharmers will go to get your private information. The advantage that pharmers have over phishers is

that whereas phishers have to get their prey one by one, pharmers can get a whole bunch of individuals at a time.

6.3.3 How Pharming Works

On a very basic level, a pharmer can work through a Trojan horse. Once a "relevant" Trojan is installed on the host computer, it rewrites the local host files on the computer. What a host file does is convert a URL into a numerical string that your browser understands and takes you to the Web site. However, a compromised host file can direct you to a malicious Web site even if you type in the right URL.

The more enterprising pharmers use a technique called DNS poisoning. DNS translates all Web addresses to numerical strings. It's sort of the telephone directory of the Internet. Now if the DNS directory is "poisoned" or altered in any way, all the users who key in the URL for a particular Web site will be herded off to a bogus site. This is a much scarier scenario. Just imagine if your online banking site were to be poisoned: everyone who would access any information on the site to make any for of transaction would be "sharing" his information with a pharmer.

6.3.4 Stopping Pharmers

Pharming is the work of hackers of some calibre. It is a pretty difficult thing to do, and that's why it's a pretty difficult thing to detect. Pharming requires the knowledge of how to manipulate DNS caches, or gain access to someone's computer files or corporate servers to change settings. Stopping pharming is not an easy task. However, there are some ways one can guard oneself against pharming.

❍ As always, keep your anti-virus and anti-spyware scanners up-to-date.

❍ Check whether the site you are sending confidential information is on a secure connection, i.e. check whether the URL is an HTTPS rather than a HTTP.

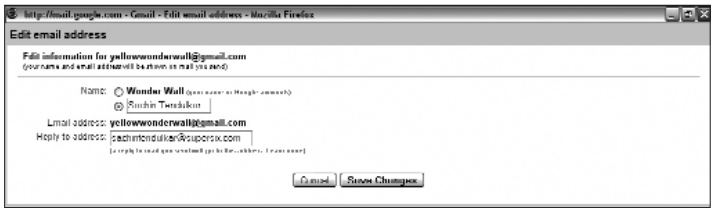
❍ From the view of the site owners, it is imperative that they keep several intrusion barriers to their DNS servers, which will stop pharmers from making malicious changes to their sites, and will prevent users from going to a malicious site.

❍ There is a simple procedure that can help you detect whether a site is legitimate or not. At a command prompt, type in "nslookup" (without the quotes) followed by a space and the IP address of the site that you find questionable. To make sure the site you are viewing is legitimate, check the domain name that comes up after this process.

6.4 E-mail Spoofing

Put simply, e-mail spoofing implies changing your name in an e-mail so it looks like the e-mail came from someone else, or somewhere 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.

Spoofing is a relatively simple exercise. In fact, one can do this very easily, at a smaller level, with one's own e-mail client / provider. Just go to the Settings option of your e-mail client, and in the account information field, change the name that the receiver will see in the e-mail, and change the Reply-To address.



Spoofing is actually very simple!

6.4.1 How It Works

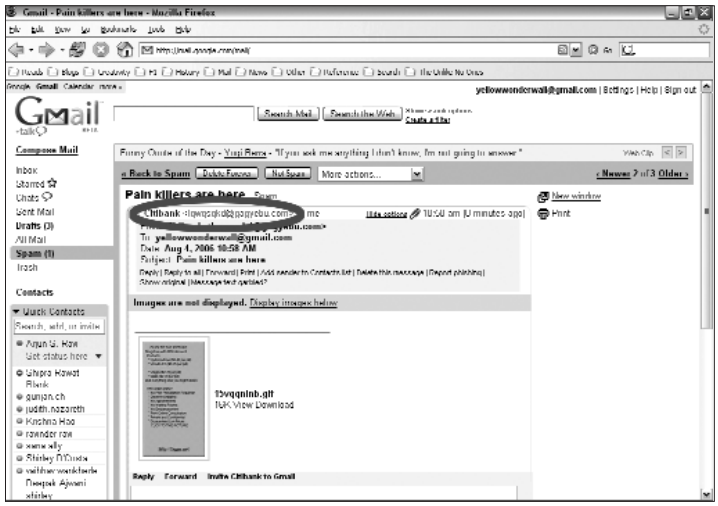
Spammers these days are using more and more complex methods to hide their identities and to send e-mails from a host of wholly random e-mail addresses. Using e-mail clients to disguise the origins of e-mails has become somewhat naïve as users and e-mail hosts are becoming quick to spot fakes.

Most spammers these days use worms to do their dirty work. After infecting a host computer, the worm searches the address book of the e-mail client that the host is using. Then, it uses those addresses in the "From" field of the e-mail and sends the spam to the rest of the users in the address book. Some of the smarter worms have random word generators and inbuilt word lists that are used to change the address of the sender.

6.4.2 Telling A spoof

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.

❍ Even if the name of the sender appears to be legitimate, check



Citibank doesn't have such a cryptic mail server

the "From" address. More often than not, with spammers using randomly generated e-mail addresses, it is likely that the "From" address will be a jumble of words.

❍ If the e-mail claims to be from a corporate source, check the SSL certificate of the mail to ensure that it is from the source it is supposed to be from.

❍ If you receive a bounced e-mail with either a virus attachment or some links to malicious sites, you know that someone's computer has been hijacked by a worm that is sending out e-mails using your e-mail address.

❍ 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>shwideoifj>AccountMaintenance-dnif82jr-4md>gobargas.co.in**) then the links are probably fake.

❍ However, if the mail is in HTML, then the link can easily be cloaked. In such an instance, an easy way of checking where the URL will take you is by hovering your mouse pointer over the link and checking the link that is shown in the status bar of your browser.

❍ Apart from this, do the same checks that you would do to check whether the e-mail was from a phisher or a spammer.

6.4.3 Stopping Spoofs

Most spam filters and e-mail providers catch common spoofs with reasonable accuracy. One of the main steps towards this direction is the Sender Policy Framework (SPF). What SPF does is that it allows the owners of domains to identify their outgoing mail servers in DNS *(see 6.3.1)* and then the mail servers check the addresses in the mail headers against the DNS to determine whether the address is genuine or spoofed.

Microsoft has taken this forward with the concept of Sender ID, which is to e-mail what caller ID is to a phone. The Sender ID concept works on the basis of the IP address of the sending server, which is checked against a registered list of servers that the domain owner has authorised to send e-mail. This verification is automatically checked, before the mail is delivered, by the ISP or the mail server of the recipient.

6.5 Pretty Good Privacy

No method of protection is absolutely foolproof. However, a big step in ensuring e-mail protection is PGP or Pretty Good Privacy. PGP is essentially a data encrypting program which provides privacy and authentication. The theory behind it is that messages are encrypted so that no one but the intended receiver can decrypt them.

PGP can technically be used to encrypt any form of data. However, it is most commonly used for sending e-mails and Internet fax.

6.5.1 How it works

Essentially, PGP works like a coding machine from those early war movies. It codes the message into an algorithm that can only be decoded if the same passphrase that the coder used to code the message is used by the decoder. The software makes use of keys and "keyrings". Keys are basically of two types—public and private. The public key, as the name suggests, is basically the location of your mailbox. PGP allows you to send the public key to whoever you like (hence the term "public"). So anyone who has the public key knows the location of your mailbox and can send you e-mails at the key address. However, only those who know the private key can open the message and read it.

Using a simple analogy, the public key is the address of your home. Anyone can send you letters using that address. These let-

Each participant in your e-mail loop needs a key.jpg

ters are slipped under your door or into your mail tray. Only those who have the key to the lock of the door (i.e. the private key) can open the door and read the message.

Hushmail offers free encrypted e-mail

PGP encrypts messages sent from your computer to a designated recipient. The private key of the recipient decrypts the message, which also contains the "session key", that is, the key for that particular mail session, to read the e-mail. In this way, PGP provides a very high level of security.

6.5.2 Using PGP

Sending an encoded message using PGP is actually quite simple. If you have the public key of the person you want to send the e-mail

to on your "keyring", you can use your mail client to send it to that location. If you don't have the public key, you can ask the person to mail it to you, or you can just search for it on the hundreds of public key servers available online.

Once you have the key, you get onto your e-mail client, type in your message and select "Encrypt" (or "Confidential") from the PGP menu. The program will ask you for your passphrase, and will encrypt your message. For the receiver to read the message, he will have to choose "Decrypt" (or "Verify") from the PGP menu and then, key in his passphrase.

6.5.3 Hushmail

An alternative to PGP is a service called Hushmail (**www.hushmail.com**). It is similar to standard free e-mail services. However, Hushmail offers a high level of security given its encryption. The best part about Hushmail is that you can use it from anywhere, that is, like Gmail and the others, you can sign in from any computer connected to the Internet. All you need to know is your private/secret key.

Security On The Network

Unlike the Internet, your Local Area Network or Wi-Fi Network is a tamer beast! It is, however, not immune to being compromised. Ensure that all systems on your network are patched and updated with the latest OS updates, anti-virus, anti-spyware and anti-adware definitions. Then use the following to secure your network and Internet Access

7.1. Upgrade To XP Service Pack 2

If you haven't yet updated your machine to Windows XP Service Pack 2 (SP2), do that now. Some programs—especially those that access the Internet in the background—will get broken due to the SP2 update. This is intentional. SP2 includes the Internet Connection Firewall, which blocks most TCP/IP ports. If your application uses a port not recognised by Windows, you will need to open the port for that application.

To find out what version of Windows XP you are using, right-click My Computer and select Properties. In the General tab of the System Properties dialog box, look for the description under System; it will tell you the version of the OS along with Service Pack information. If your computer does not have SP2, you can automatically update the software by visiting **http://windowsupdate.microsoft.com**.

SP2 is, however, a huge download. It's a somewhat complex upgrade. It could possibly cause your system to crash, and you could be left without a PC for days. You'd be better off contacting a professional who can do it for you in a day rather than be stuck with a failed upgrade.

If you plan to do it on your own make sure you follow the following steps:

1. Update your virus/adware definitions and scan your entire system.
2. If you have a software firewall, get the latest version. This will be SP2-compatible.
3. Get hardware driver updates from the manufacturers of all your hardware devices.
4. Back up all your software to CD/DVD.
5. Create a system restore point.
6. Restart your computer, disable anti-virus software and all other software that are currently running, make sure you are disconnected from the Internet, and only then access the SP2 update.

7. Once SP2 is installed, reboot your system normally, let all the background programs (including anti-virus programs) load, and then connect to the Windows Update site for any fresh updates. Install those as well and reboot.
8. Last but not least, find a Windows guru (there are many on the Digit forum (**http://www.thinkdigit.com/forum**) who will be quick to help) just in case something goes wrong.

7.2. Enable Internet Connection Firewall (ICF)

For computers directly connected to the Internet, ICF is the primary level of protection offered by Windows. Unless you are using a third-party firewall, ICF should be enabled for all computers that connect to the Internet directly or indirectly (through another computer) through a wired or Wi-Fi LAN.

Make sure the Internet Connection Firewall in enabled

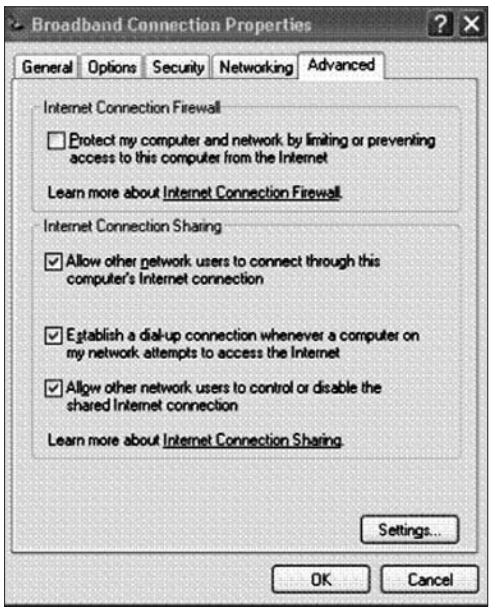
To enable ICF, right-click the Internet or LAN connection in Network Connections, select Properties, and click on the Advanced tab. Check the "Protect this computer..." box.

Note that ICF is a basic firewall, and offers only a minimum level of protection. For better protection, consider the free or paid versions of Zone Alarm (**http://zonelabs.com**) or Kerio Personal Firewall (**www.sunbelt-software.com/Kerio.cfm**). There are many more out there, but these are two of the best ones.

7.3. Enable Internet Connection Sharing (ICS)

If you want to connect multiple computers on your LAN or Wi-Fi network to the Internet, use ICS rather than having an individual connection for each computer. The computer with ICS enabled, known as the ICS host, should be connected to the Internet. This will limit your network's exposure to the Internet to only the ICS host.

To enable ICS, right-click on the Internet connection in Network Connections, select Properties, and click on the Advanced tab.



Use Internet Connection Sharing

In the section called "Internet Connection Sharing", check the box that says "Allow other network users to connect to the Internet through this computer's Internet connection". The other two checkboxes determine whether your Internet connection should dial up automatically to the Internet if users attempt to access it from their computers, and whether they should have control over sharing or disabling the ICS connection. Note that for automatic dialup, you will need to save the password for your dialup connection.

7.4. Safe Sharing On The LAN

In Chapter 2, we recommended that you turn off Simple File Sharing on a standalone home PC. While the recommendation still holds if your PC is a standalone machine with just an Internet connection, you may need to turn on Simple File Sharing if you are on a network. Simple File Sharing is standard in XP Home and available in stand-alone non-domain XP Professional systems. XP Professional has the option of using advanced file sharing even if the system is not connected to a domain. File sharing on a network can make things much easier. For example, sharing your MP3 collection folder or your family album across multiple computers at home is a much better idea than copying the same files over and over again from one computer to another.

Note that the "Simple" in Simple File Sharing refers to the ease of use in file sharing, and does not mean that the file sharing is technologically inferior to the advanced file sharing in XP Professional. Simple File Sharing hides the complexity of managing users and permissions for newbies.

To turn on Simple File Sharing, go to **My Computer > Tools > Options**. Select the View tab and check the box that says "Use Simple File Sharing (Recommended)".

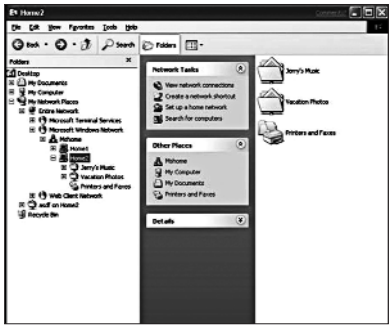
In Simple File Sharing, users have only two options:

- Share a folder on the network
- Allow users to change files in the shared folder

It is advisable to keep the shared folder in your My Documents folder or on your Desktop: it will be easily accessible, and you can disable sharing at any time you want. To create a shared folder, right-click on an existing folder, or create a new one and then right-click it. Select "Sharing and Security" to open the Sharing tab of the folder's Properties dialog box. In the "Network sharing and security" section, check the box next to "Share this folder on the network". However, the files within this folder are read-only,

that is, users cannot change the contents of the file and save it back to the shared folder. To allow network users to change the file contents, check the box next to "Allow network users to change my files". This will make this folder accessible to whoever browses the network for shared folders.

If you want to give a different name for the shared folder, type in that name in the "Share Name:" field. For example, if your local folder is called "My Music", you might want to change the name to "Family Music Centre". To verify that the files have been shared, go to My Network Places and look for the shared folder name, in our case, "Family Music Centre", under your computer name.



Network sharing of folders

If the sharing option isn't available, you'll see a message at the bottom of the Sharing tab, which says that remote connections are disabled until you run the Network Setup Wizard. Run the Wizard to set up your network, then come back to this tab to set up the shared folder.

XP Professional supports more advanced file sharing, which gives you greater control over who can access your files and what each user or user group can do with those files. To use the advanced sharing options, you will first need to turn off Simple File Sharing by doing the reverse of what's been described above.

As with Simple File Sharing, right-click on the folder you wish to share and select "Sharing and Security". The sharing tab will look different from the one with Simple File Sharing turned on.

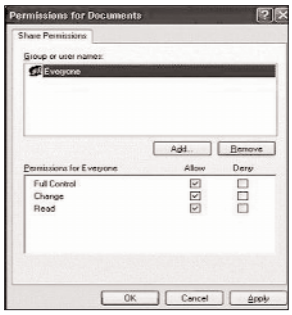
Specify a share name and click Permissions to edit the users or user groups who will have access to this shared folder. Users

(or user groups) can be given full control, permitted to change files, or only given read rights. By default, if the user is not listed in the permissions list, he will be denied access.

XP Professional's Advanced File Sharing

In the permissions dialog box, the default listing will be for the "Everyone" group. This allows access to anyone who connects to this shared folder.

Select the Everyone group and click Remove. Next click Add to select the users who can access the folder. In the resulting "Select Users or Groups" dialog box, click "Object Types". This will open the Object Types dialog box. Clear the checkboxes next to "Built-in Security Principals and Groups". Ensure that the box next to Users is checked, and click OK.

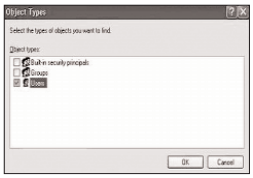


Setting Permissions for different users

Now click on Advanced and then Find Now. XP will search the network for users. Select the users to whom you want to give access to the shared folder and click OK. Double-click on each user and determine the permission level—full control, change, or read. "Full control" allows the user to make changes

and even delete a file; "change" only allows the user to change the contents of a file; and "read" restricts the user to only viewing the contents of the file.

Note that you can only set permissions if you are using an NTFS-formatted disk partition.



Users Group Selection

7.5. Securing your Wi-Fi network

Wireless networks give you the convenience of not needing to remain in a fixed location when accessing the network or Internet. However, most home Wi-Fi networks are configured for open access by default. This lets anyone with a Wi-Fi enabled laptop or PC within reception range of your access point to use your wireless network without your permission. This can be harmless but expensive "bandwidth stealing" where they "piggyback" on your network to access the Internet. They could also use it for malicious purposes like using your machine and network as a zombie to attack other sites or even scan your system for personal data if your wireless network is left unprotected. Additional steps therefore need to be taken to protect your wireless network from hackers and unauthorised users.

There are three steps involved in securing a wireless network:

❍ Authentication: Before data is exchanged, wireless devices should identify themselves and submit appropriate authentication credentials.

❍ Encryption: Before data is sent, the wireless device should encrypt it to ensure no-one else can read the transmitted data.

❍ Data Integrity: Sent data should contain information that the receiver can verify and thereby confirm that the data was not modified while in wireless transit.

7.5.1.Set Up A Secure Wireless Home Network

In order to set up a secure, wireless home network, you will need to do the following:

Pre-Installation Checklist

Prior to installation, you will need:

1. A USB pen drive with at least 2 MB of free space.

2. A wireless Access Point (AP) or router connected to your LAN or Internet connection. Check the AP vendor's documentation on how to physically connect the device. Do not configure the AP at this point.

3. To determine which of your wireless devices (laptops, PCs etc) support Windows Connect Now technology.

4. To determine which method of authentication and encryption is supported by all your wireless devices including the AP, lap tops, PCs, etc. The wireless devices must support either WPA-PSK/TKIP, which is the recommended protocol set, or open sys tem/WEP. The latter is discouraged as it is a weak-security sys tem. You will need to use open system/WEP if some of your devices do not support WPA-PSK/TKIP.

5. To ensure that if the computers have an external switch to turn on the wireless adapter, they are indeed turned on.

6. To ensure that Windows XP has been updated to Service Pack 2.

7. To configure all the wireless computers in your network for automatic addressing. To do that, open Network Connections, and under Wireless Connection, right-click and select Properties. Under the General tab, in the section "This connection uses the following items", select Internet Protocol (TCP/IP) and click Properties. In the resulting dialog box, under

the General Tab, select "Obtain an IP address automatically" and click OK twice.

8. To enable automatic wireless network configuration. To do that, right-click on the wireless connection and select Properties, select the Wireless Networks tab, ensure that the box that says "Use Windows to configure my wireless network settings" is checked.

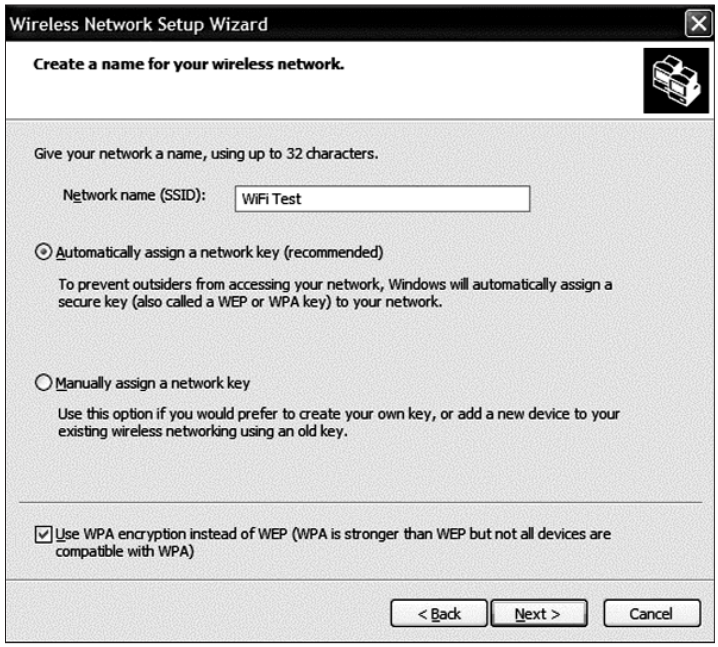
Installation

If possible, start the Wireless Network Setup Wizard on a computer that is connected to a printer, so you can use the configuration information printout to manually configure wireless devices that do not support Windows Connect Now technology.

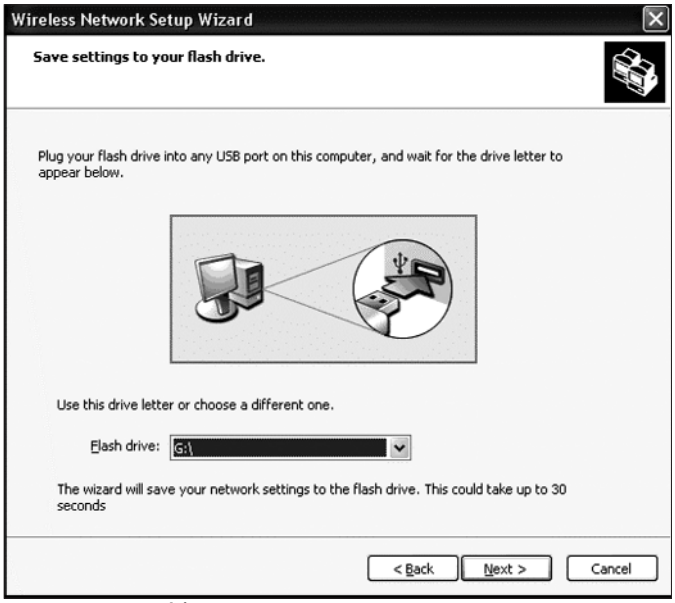
Use the Wireless Setup Wizard

1. Open My Network Places, and in Network Tasks, click “Set up a wireless network for a home or small office”. This will launch the welcome page of the Wizard. Click Next. (In some cases you may be redirected to the Network Setup Wizard, which will ask you to provide an Internet connection method, a name for your network workgroup, and whether file and printer sharing should be enabled for the network. You will need to complete these tasks before you can resume setting up the wireless net work).

2. If this is the first time the Wizard is running, a page will be displayed asking to create a name for the network. In the “Network Name” field, type a name for your network. Select “Automatically assign a network key (recommended)”. If all your wireless devices including the AP support WPA, check



Network Name and Encryption Selection



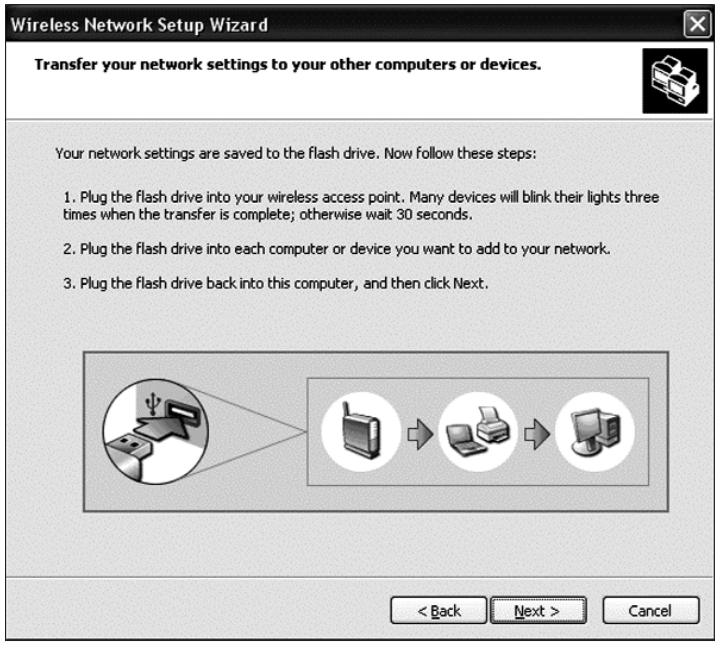
Insert a USB Pen drive

the box that says "Use WPA instead of WEP". (If the Wizard has been run before, you will asked "What do you want to do?" Select "Set up a wireless network for a home or small office", and click Next.)

3. You will be asked how you want to set up your wireless net work. Select to use the USB Flash drive option and click Next.

4. The Wizard will now ask you to plug in your USB drive. When you insert the drive, it will be automatically detected, and the drive letter assigned to the pen drive will be displayed. Click Next.

5. The Wizard will copy all the necessary files to the USB drive, and then display a page asking you to transfer the settings to other computers and devices. Do *not* click Next at this time.



Transfer Wireless Setting to the Pen Drive

6. Take the USB drive and plug it into your Windows Connect Now enabled Wireless Access Point. If your AP does not support Windows Connect Now, skip this step. If there is a read-out display, select the options to complete the configuration. If there is a no read-out display, the indicator panel should have a green LED that flashes three times when configuration is complete. Some AP vendors use the LED indicators for other purposes, so be sure to refer to the documentation. In any case, leave the USB drive in for at least 30 to 60 seconds to ensure that the network configuration is updated to the AP.

7. Follow the above procedure if you have any other wireless devices (such as printers) that are Windows Connect Now capable.

Launch the Wireless Client Setup

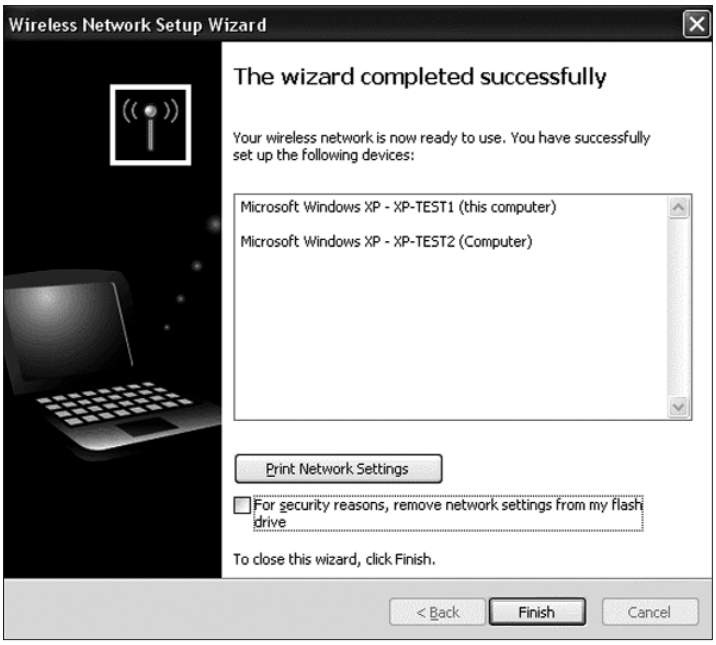
8. Plug the USB drive into your other wireless Windows XP SP2 computers, that is, other than the ones where you created the wireless setup configuration. The Removable Disk dialog box will open with various options; select "Wireless Network Setup Wizard using the program provided on the device" and click OK. (If the Removable Disk dialog box doesn't start, open your USB Drive from Windows Explorer, find the file setupSNK.exe, and double-click it).

9. You will be prompted to add the computer to the wireless net work. Click OK. The wizard will now configure your computer for wireless access. When it informs you that the computer has been successfully added to the wireless network, click OK.

10. Follow the same procedure for all your other Windows XP SP2 computers.

11. Plug the USB drive back into the original computer (where you created your wireless network configuration in Step 5). We had left the screen at the "Transfer your network settings to your other computers or devices" page. Click Next.

12. The setup Wizard will now display all the computers and devices configured for wireless access. Click the Print Network settings to print out the settings that were used to configure the wireless network. Use this printout to manually configure those devices that are not Windows Connect Now capable. If you want to keep the wireless settings on your USB drive for later use, clear the checkbox next to "For security reasons, remove network settings from my flash drive", else remove the settings from your USB drive by leaving the box checked. The latter is recommended

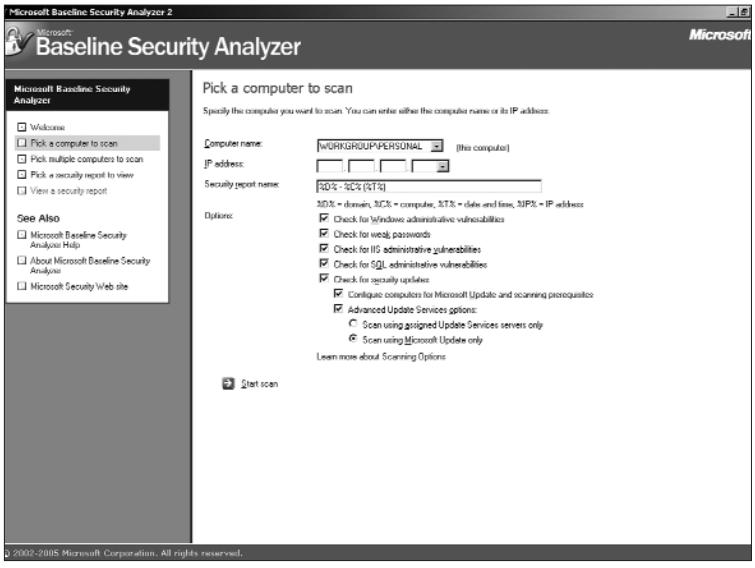


Take a printout of the settings for Manual Configuration later

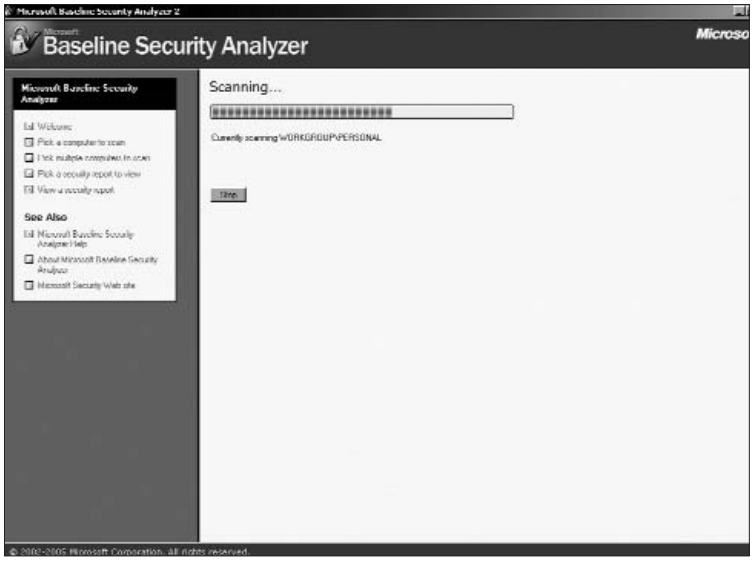
as it is more secure. Click Finish. Your wireless network is now secured and ready! The WPA encryption will ensure that all wireless transmissions between your various Wi-Fi devices are encrypted and that no unauthorised users will gain access to your network.

7.6. Verify system security with Microsoft Baseline Security Analyzer (MBSA)

A very useful tool that will save you time and help you in bullet-proofing your network is the Microsoft Baseline Security Analyzer tool. It will scan for common security misconfigurations and missing security updates for all the computers on your network. It has an intuitive interface and informative dialogs, and gives a detailed report of the security vulnerabilities that your computers are exposed to. It will show you what



Scan a computer for security holes

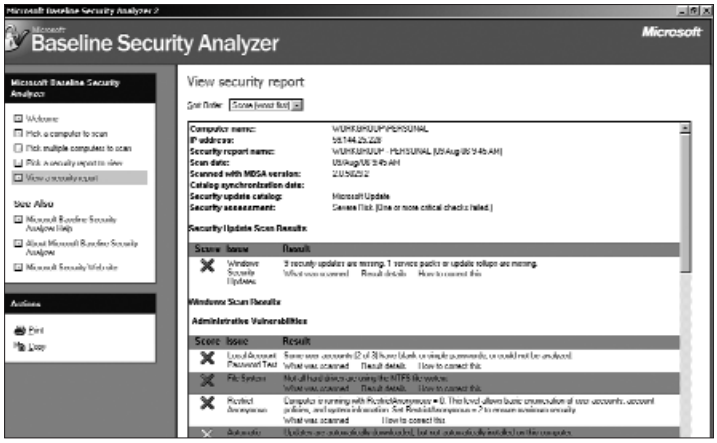


The MBSA Scanning in progress

was scanned, what the results of the scan are, and what the steps to correct the vulnerabilities are.

Get MBSA by visiting **www.microsoft.com/technet/security/tools/mbsahome.mspx**. The latest version is MBSA 2.0. Download, install and launch the application. You can choose to scan either a single computer or multiple computers. For scanning multiple computers, you will need to specify a Workgroup or Domain name, or give an IP address range that covers all the computers on your network. You can also scan one computer at a time.

Select all the checkboxes including the "Advanced Update Services options" box. Under this, select the "Scan using Microsoft Update only" radio button. Then click Start Scanning. MBSA will connect to the Microsoft Web site, download the latest security update catalogue, and then start scanning your system(s).



Use the scan report to fix security holes

Once the scan is complete, you will get a detailed listing of all the security problems on your computers in the net work, along with the details of the recommended actions to correct them.

Once you've rectified the problems identified in the MBSA report, run another scan to make sure you get a clean bill of health.

Going Online

Amidst all this talk, there have been the good guys—anti-spyware tools and such—and the bad guys: the spammers, the phishers, and such. Each of these sides is constantly battling the other. With all this action going on, where exactly do you and every other average Joe Internet-user stand? What should you do before you take that giant leap online? Read on...

8.1 Browser Security

The Web browser is your portal to the big bad world that is the Internet. It's also the easiest way a hacker, spammer, or phisher can attack your computer. An unsecure browser therefore means that the door is open for those with malicious intent to get into your computer, all guns blazing.

Part of the problem is that some Web sites have content that can only be viewed if you install additional software, which puts your computer at further risk of attack. But before we go into how you can effectively secure your browser, let's take a look at what features hackers are looking to exploit.

8.1.1 Getting To Know Your Browser

Why you need to know what you're doing with your browser is that you could inadvertently install a feature that makes it less secure.

Here's a look at the common features that Web browsers have to view content on the Internet. These are common across almost all browsers.

❍ **ActiveX**: A technology used by Microsoft IE. It allows different applications, or parts of applications, that you have installed on your computer to be accessed by your browser to display content. These applications may already be in your computer, or they may have to be downloaded. This is where the security threat comes in, because if the ActiveX controls aren't properly implemented, your computer will become seriously vulnerable.

❍ **Java**: A language used to develop content for, among other things, Web sites. Content in this case is interactive, wherein there is usually some input from the user. The Java Virtual Machine is used to view Java applet on sites. If you have come across Java content and it played in your browser, you have the JVM installed;

❍ **Active Content**: This is generally enabled by plugins installed on your browser to view interactive or dynamic content such as

videos and animations. An example is the Macromedia Flash plugin, which allows you to watch Flash animations.

❍ **JavaScript**: A language used to develop active content for Web sites. For example, JavaScript programs certain images on Web pages to change into other images as the mouse cursor is moved over them.

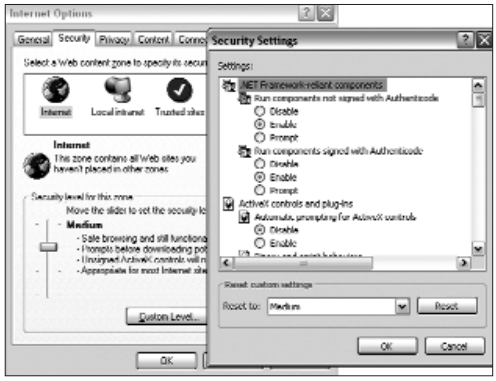
❍ **Cookies**: Text files on your computer that store data used by Web sites. Cookies can contain any form of information that the Web sites have designed for them.

You're now ready to get your browser secure.

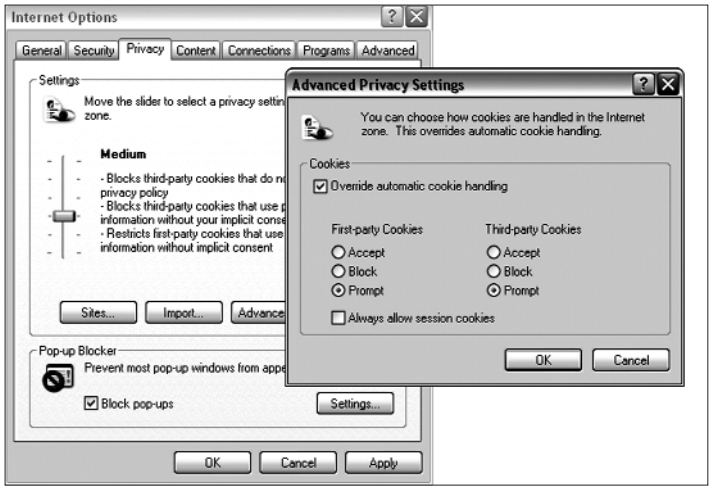
8.1.2 Microsoft Internet Explorer

IE is one of the most popular browsers, mostly because it comes bundled with Windows. Since a large number of individuals use this browser, a large number of hackers make it their target. IE makes use of ActiveX content, and this, in a large number of cases, makes it very vulnerable to outside attack. Ideally, you should disable all features that have the smallest chance of placing your computer at risk. However, here are some smarter options.

The first thing you should do is to check your IE security settings. You can access this option from **Tools > Internet Options > Security**. If you are an average Internet user and have a decent anti-virus on your



You can choose a security level depending on the type of internet usage

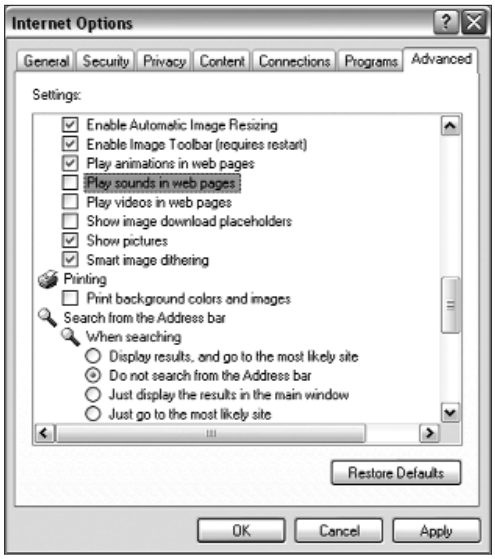


Get IE to prompt you for cookies

computer, we recommend the Medium security setting for the Internet zone (IE has security settings for various zones—the Internet, Local Intranet, Trusted Sites and Restricted Sites). You can choose to select certain functionalities through the Custom level button, which shows you the various features you can enable or disable depending on your requirements. For example, you can enable Automatic Prompting for ActiveX controls, which gives you the option of being prompted every time an ActiveX control needs to be installed. You can also change settings for accepting downloads, installing items on your desktop, using the pop-up blocker, and more.

In the Privacy tab, you will find your computer's settings for cookies. Here's an example of just how much control you can have: if you are *really paranoid*, press the Advanced button and select "Override automatic cookie handling". Select Prompt in both fields. This will give you an alert every time a Web site attempts to place a cookie on your computer. You can then choose what you want to do with the cookie.

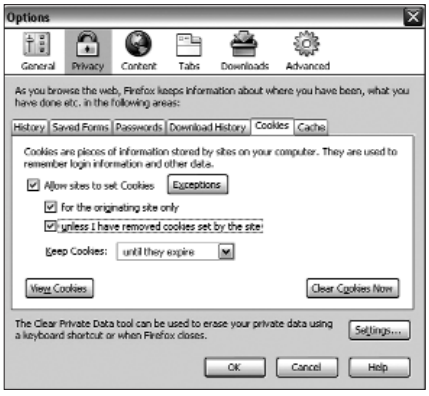
Ideally, you should disable IE playing sounds and video on your browser as these are potential vulnerabilities. Select the Advanced tab, scroll down to Multimedia Options, and deselect the items of your choice.



Disable multimedia options on IE

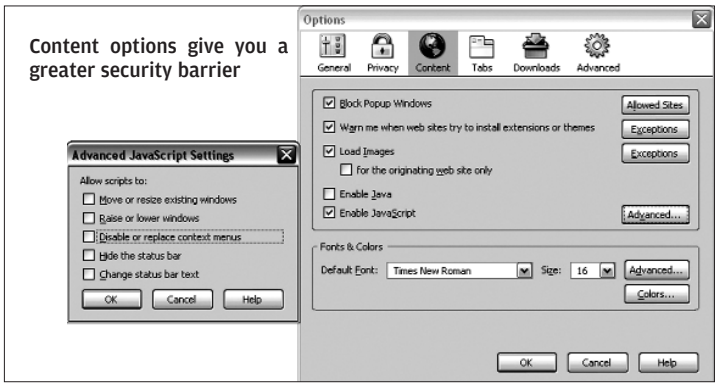
8.1.3 Mozilla Firefox

Firefox has almost the same options as Internet Explorer. It does not support ActiveX, though, and the security options are not on the basis of zones. The development model that Firefox is based on however, is much more secure than that of IE. It is recommended that you first look at **Help > For Internet Explorer Users**, so you get a hang of the differences in terminology.



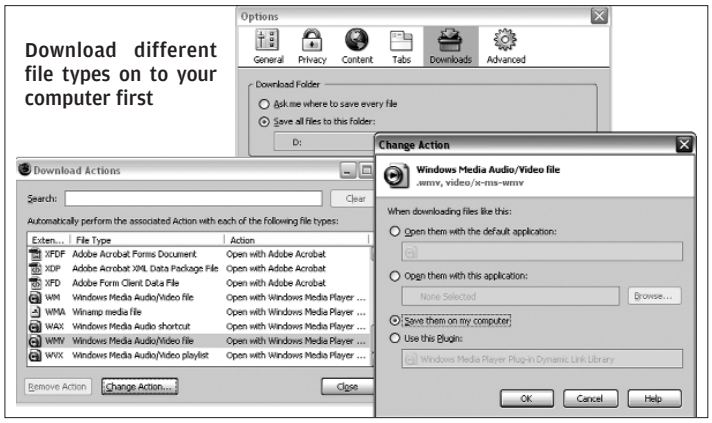
Edit your cookie options for Firefox

To edit Firefox security options, select



Tools > Options. Now, as with IE, go to the Privacy tab. Here you will find options for, among other things, Cookies. Under the Cookies tab, it is recommended that you enable cookies only for the originating site. It is also recommended to select the "unless I have removed cookies set by the site" option, in which case a Web site will get blacklisted from setting cookies on your computer if you have removed them manually.

The next security area is the Content tab. Under this, select the Block Popup Windows option, the function of which is self explanatory. Also select the next option, that is, "Warn me when

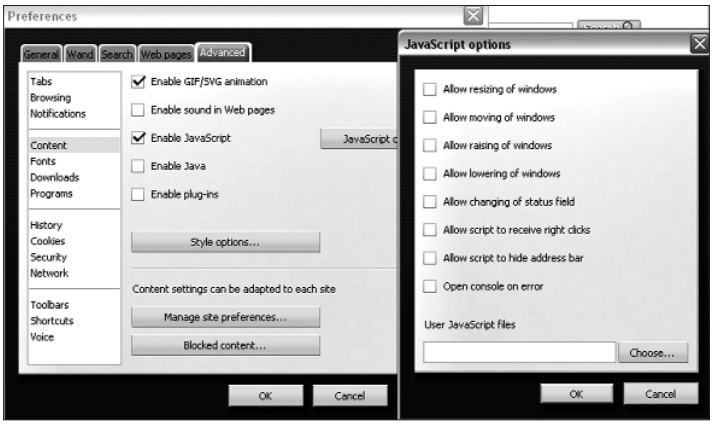


Web sites try to install extensions or themes". The most important option here is the Enable Java option. It is recommended that you *not* check this option. This is because Java allows Web sites to run applications on your computer, increasing the vulnerability of your system. Anytime you wish to view the Java applets on a particular site, check the option, and remember to deselect it when you leave the site. Select the Advanced button in the Enable JavaScript option. We recommend that you disable all the features mentioned here.

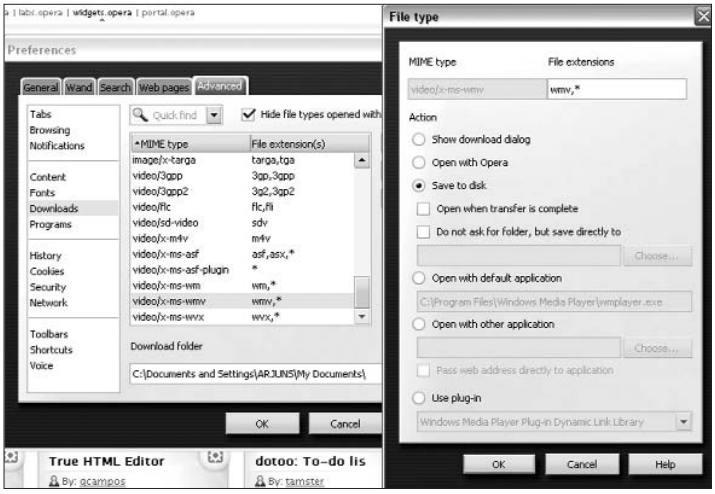
In the Downloads tab, click the "View & Edit Options" button. The Download Actions box that opens shows different file types and the actions that Firefox will take when dealing with these file types. For any file type, click the Change Action button. In the Change Action box, select "Save them on my computer". This is the secure option, since when the files are opened from your computer, your anti-virus will detect whether there is any hanky-panky or not, if it hasn't already when you visited the Web site.

8.1.4 Opera

The latest version of the Opera browser comes with added functionalities and security measures. View the current options the



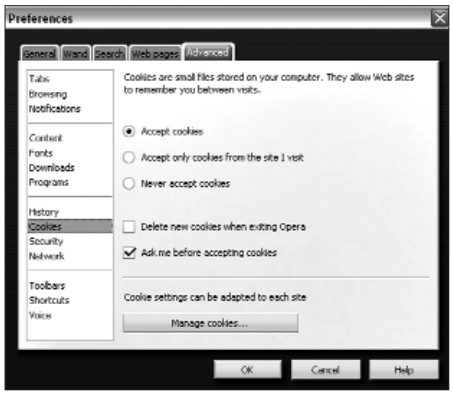
Keeping Opera secure



Save different file types to disk

browser is using by going to **Tools > Preferences**. In the General options tab, select "Block unwanted pop-ups" in the pop-ups drop-down.

Next, click on the Advanced tab. Here, select the Content option. Like with IE and Firefox, disable the Java option. In the JavaScript Options box, disable all options. Also disable the "Sounds in web pages" option.



Let Opera alert you when there is a cookie around

In the Downloads option, choose a file type and click Edit. In the file type box that opens, select "Save to disk".

Like with Firefox, you can get Opera to alert you when a Web site is attempting to set a cookie on your computer. You can do this by checking the "Ask me before accepting cookies" option in the Cookies tab. Once again, use this option if you are really fearful of being attacked.

Block pop-ups with Opera

8.2 Firewalls

A firewall is based on a security policy—which can be customised by the user—that permits or denies communications to and from your PC. The difference between a firewall and an anti-virus is that a firewall blocks access to your computer and the setting up programs there, while an anti-virus blocks different kinds of security threats like virus installations and other malicious content where the presence of physical outsider access is not necessary.

8.2.1 The whats, whys and hows

Basically, a firewall protects your computer from unwanted Internet traffic. It filters the information coming into your computer, and if the information does not pass through the filters, it is blocked from entering. There are essentially two types of firewalls—personal (software) and network (hardware). We are here only discussing personal (software) firewalls.

A personal firewall allows you to request whatever you like from the Internet, but it blocks attempts to access files, applications, etc. on your computer. This is done in one of three different ways depending upon the firewall in use:

❍ Packet filtering, wherein packets (small chunks of data) are put through your firewall's filters. The filters decide whether the packets are to be accepted or not.

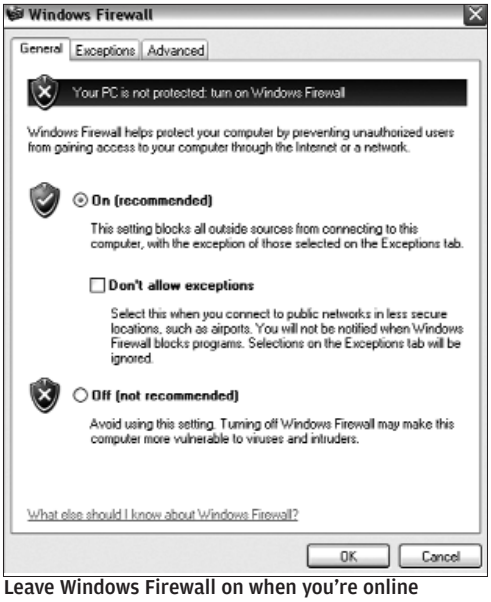
❍ Proxy service, wherein the firewall makes the Internet requests rather than the computer itself. The data that the firewall retrieves is then sent to your computer.

❍ Stateful inspection, wherein only certain parts of packets are analysed by the firewall. This is done by comparing these parts to a database of trusted packets.

But why do you need a firewall when you already have an anti-virus? Well, there are some functionalities that only a firewall can provide. For example, a firewall protects your computer from the threat of remote logins. Effective firewalls can block access to files and applications on your computer that others may be trying to access. Firewalls also protect against application backdoors: some applications have features that allow remote access, and these act as backdoors to your computer that hackers try and exploit.

8.2.2 Which Firewall?

XP comes with an inbuilt personal firewall. The firewall is enabled by default. It can be accessed through the Security Center in the Control Panel. It is advisable to turn it on and leave it on while you are connected to a network.



Leave Windows Firewall on when you're online

There are also several third-party

firewalls you can use, which have more functionality than Windows' inbuilt firewall. Some of the better ones are:

❍ Norton Personal Firewall: It's almost a rule of thumb—all Symantec products are trustworthy and reliable. The Norton Personal Firewall is no less. It has a very easy-to-use interface and offers various levels of security with different options for each level. However, it is quite expensive, at $49.99 (Rs 2,250).

❍ ZoneAlarm Pro: One of the best-known firewalls in the market today. The interface is very clean, and it offers one of the best firewall protections that money can buy. It comes with a host of security features, and is more a security suite than just a firewall. It costs $39.95 (Rs 1,800) for one year for one PC; however, you can download the free version of the software, which offers very basic firewall features.

❍ Comodo Personal Firewall: This is a free personal firewall that is almost as good as the ones you have to pay for. Comodo features pop-up warnings that identify over 7,000 programs as safe (elsewhere seen only in ZoneAlarm Pro) so they don't persistently annoy you with warnings. However, it is meant only for Windows 2000 and Windows XP SP2.

8.3 Anonymous Surfing

We mentioned how firewalls can also act as a proxy service wherein the firewall essentially retrieves requested information on behalf of the user. This takes us to the concept of anonymous surfing.

As the name suggests, anonymous surfing is surfing the Net without your identity being disclosed (by hiding your IP address) to the Web sites you are visiting. Anonymous surfing works on the platform of proxy connections. This means that you are accessing the internet through a proxy server. A proxy server takes your internet requests (in the form of URLs) and retrieves the information through itself rather than through your computer. This retrieved information is therefore not displayed on

your computer directly from the Web site itself, and you remain invisible to the site.

There are, of course, certain risks involved with using proxy servers. A malicious proxy server could record all the information you send through it. Hence, it is always better to use proxy servers that are of known integrity, like the ones we've mentioned below...

8.3.1 Free Proxy Servers

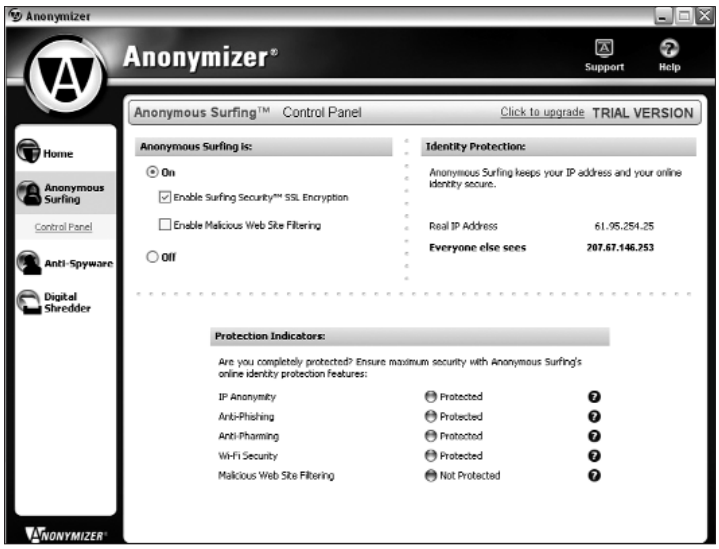
Here's a look at some of the better ones.

❍ Anonymouse (**www.anonymouse.org**): One of the simplest, free proxy servers. It does not support several links such as HTTPS, MAILTO, etc. It only hides your IP address from the Web site you are visiting.

❍ Iphide (**www.iphide.com**): Like Anonymouse, iphide too offers only hiding of your IP address from the Web sites. It is very simple to use, and offers little other than, well, hiding your IP.

Anonymouse is simple and fun

iphide is about as good as Anonymouse



Configuring Anonymizer anonymous surfing

❍ Proxify (**www.proxify.com**): At first glance, Proxify looks like a covert militant site for a terrorist outfit. But Proxify offers one of the most comprehensive, free Web proxy service available today, with a variety of options for users.

Proxify rules!

8.3.2 Anonymizer: Anonymous Surfing

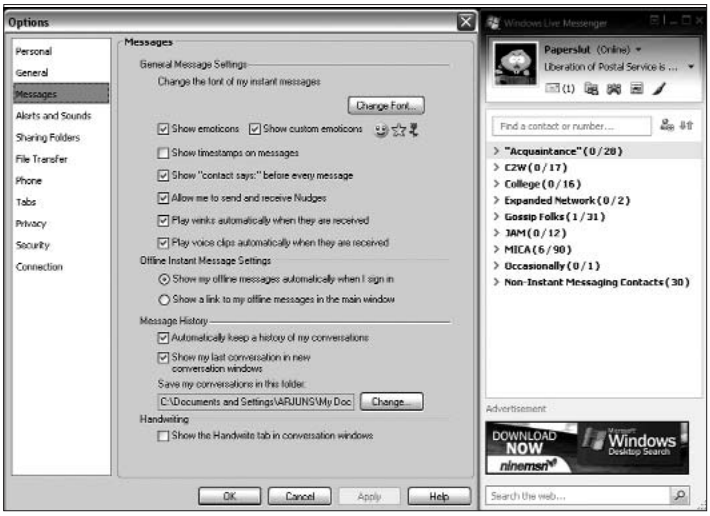
Anonymizer is one of the most effective commercially available anonymous surfing options available in the market. As an anonymous surfing suite, it has a much higher level of functionality than just a Web proxy server. As a standalone software, it not only hides your IP address, it also provides full-time SSL encryption for every transaction, giving you extra security. It comes bundled with anti-spyware options that are also very effective security measures.

8.4 Safety Over IM

Like with e-mail, instant messaging, too, suffers from the threat of malicious prowlers. IMs have become all-pervasive; this means that at every location where a user accesses his IM account, he faces the risk of being observed by a hacker. Given the different levels of security available at these areas, you never know when, or where, you might be watched.

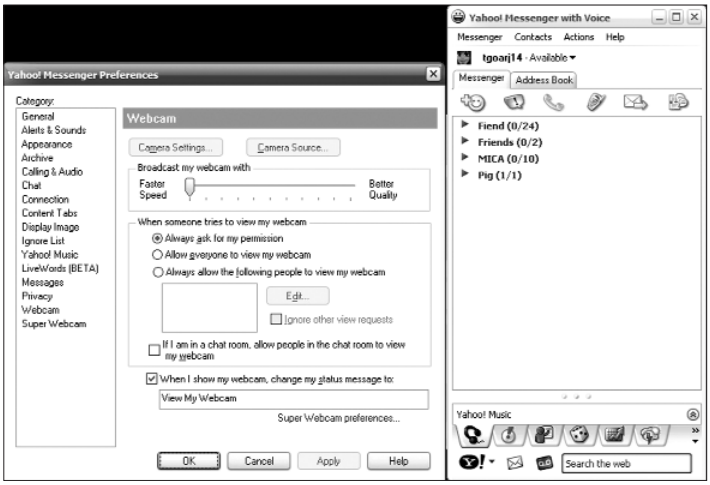
8.4.1 Safe Chatting

There are several simple things you can do to make sure your chatting experience remains safe and secure.



Disable the message history option at cybercafes

❍ Never, ever, give out personal information in a chat room, or in a chat wherein multiple individuals have the opportunity to see what you are typing. Passwords, credit card numbers, and such should not



Changing webcam preferences in Yahoo Messenger

be shared over IM unless you are more than 100 per cent sure of the trustworthiness of the receiver.

❍ Avoid using your real name as far as possible.

❍ Blocking is a very effective tool to keep away individuals who have appeared on your contact list uninvited. Use it, use it often.

❍ If you get a lot of chat spam (inviting you to view Webcams, and so forth) on your instant messenger, you can change your Privacy settings to allow only those on your contacts list to send you messages.

❍ When chatting at a cybercafé or at a location away from your home, make sure your chat logs are not being saved. You can check this in the Options menu of most IM clients.

8.4.2 Prevent Webcam Hacking

If you are used to chatting over IM with a Webcam, then you're probably aware of the fact that your Webcam can be accessed by anyone on the IM network who knows your IM username. The important thing is to stop malicious people from hacking into your Webcam. The easiest thing to do in such a situation is to disconnect your Webcam when you don't intend to video-chat. However, if you must leave it on, in the Options/Preferences menu of your IM client, change the settings so that people can only view your Webcam with your permission.

8.5 Using P2P Wisely

Peer-to-peer networks are considered by some to be the best thing to have happened to computers since the Internet. Everyone knows what they do and what they're capable of. Yet, P2P networks are also one of the biggest security threats to your computer. There are tons of files infected with viruses and distributed over these networks. However, there are a few rules you can follow to make sure you have an enjoyable and safe P2P experience:

❍ Most file-sharing applications these days come bundled with a host of adware and spyware. Make sure you know exactly what you are installing on your computer. It is advisable to run an anti-spyware application immediately after installing your P2P client.

❍ Choose your client carefully. In an attempt to provide you with more and more functionalities, a lot of P2P clients leave insecure backdoors open and also install a variety of adware on your computer, and heighten the vulnerability of your computer.

❍ Disable all "supernode" or "hub" settings. You can do this in the Options menu of your client. By becoming a supernode, your computer acts as a server for other computers in the vicinity. It performs searches for these computers on their behalf, making it more prone to attack.

❍ Remember to keep your firewall on when you're using a P2P client, even if the software warns you that doing this could corrupt your downloads.

Safety On The Go

As we increasingly tend to move everywhere with our mobile devices, hackers, too, are spreading their wings, as it were. Travellers are especially vulnerable as they tend to be less than totally vigilant about their devices. This section will look at some of the steps you can take in securing your devices from data attacks, loss, and theft when on the move.

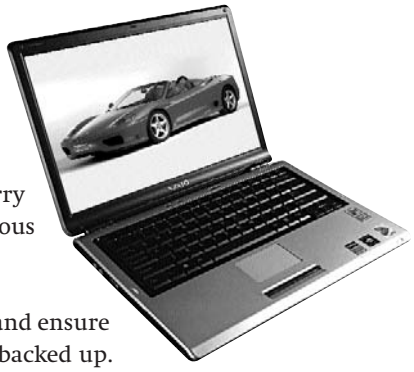
9.1. Laptop Security

Laptop theft is one of the most common of hi-tech crimes. Industry statistics estimate that well over 6,00,000 laptops are stolen every year with financial losses running into thousands of crores of rupees. When you lose your laptop, you not only lose the physical machine—you also lose the information stored on it, which in some cases could have irreplaceable commercial value. Take these precautions and protect both your intellectual as well as physical property.

9.1.1. The basics

❍ When travelling, make sure you keep your belongings in sight at all times.

❍ The same goes for conferences and meetings. Keep your laptop in view at all times. If you need to go out of the room, take it with you, or ask a colleague to keep an eye on it.



❍ If you have to go for a meeting without a laptop and want to leave it in a vehicle, keep it covered or in the boot, not in plain sight.

❍ Do not use flashy cases to carry your laptop—make it as inconspicuous as you possibly can.

❍ Have an external backup device and ensure that all important data is regularly backed up.

❍ Use a pen drive to store your sensitive data. Of course, you need to ensure that you also keep the pen drive safe!

❍ Register the laptop with the manufacturer. This will help in recovery if a stolen laptop is returned for servicing or repair.

❍ Use tracking software to have the laptop call home. While not so easily available in India, tracking software enable one to track

down laptops as soon as they connect to the Internet. The software operates in stealth mode, sending information that will be helpful to police, ISPs and security agencies in tracking down the location from where the laptop was used.

9.1.2. System-level Deterrents

❍ Use a strong BIOS password—one that is hard to guess and is not a standard dictionary term. Some laptops offer the facility of locking the hard disk as well with the BIOS password. This way, even if the thief removes the hard disk and tries to use it on another machine, it will not be accessible.

❍ Use a modern OS such as Windows 2000 Professional or Windows XP Professional. (Linux, too, though we do not cover it here).

❍ Configure your Windows system to always require a password to log in. (Go to **Control Panel > User Accounts**, and ensure that "Users must enter a user name and password is password" is checked.)

❍ Enable strong passwords. Go to **Control Panel > Administrative Tools > Local Security Policy**. In Password Policy (under Account Policies), change the value of the setting "Passwords must meet minimum complexity requirements" to Enabled. Passwords henceforth will be required to meet the following minimum characteristics:

- Should not contain significant portions of the username or full name
- Should be at least six characters long
- Should contain characters from at least three of the following four categories:
- English uppercase (A to Z)
- English lowercase (a to z)

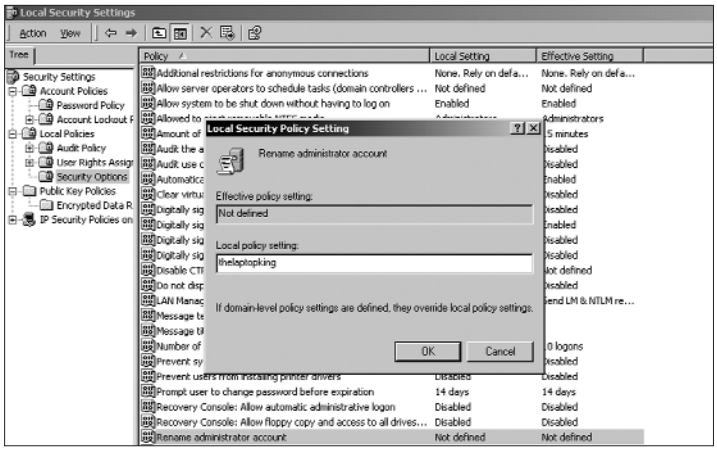
- Base 10 digits (0 to 9)
- Non-alphanumeric characters such as !, @,, #, $, %, ^, &

❍ When connecting from hotel rooms and other secure locations, your laptop will be vulnerable to hacker attacks. Use a personal firewall.

❍ Use the NTFS file system.

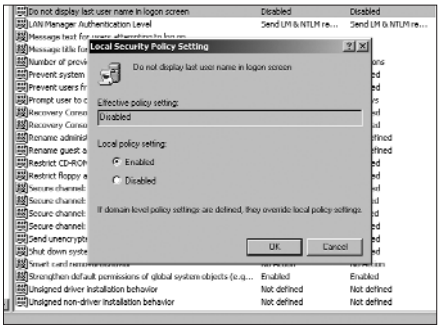
❍ Disable the Guest Account.

❍ Rename the Administrator Account, which gives users full control over the entire system. The normal name of the Administrator account is "Administrator". This is commonly known to all, and hackers will first attempt to crack the Administrator account. Renaming the Administrator account will make it harder for the hacker to figure the Administrator account name and password. To do this, go to Local Security Policy (**Control Panel > Administrative Tools**), click on Security Options in the left pane



Renaming The administrator account

under Local Policies, select the "Rename Administrator Account" setting, and enter a new name for the account. Avoid using words such as "Admin", but use an easily-remembered name.

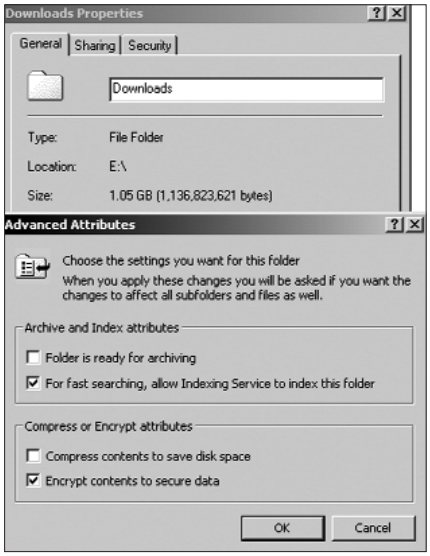


Disabling display of last logged in user

❍ Create a dummy Administrator Account. Under **Control Panel > User Accounts**, create an account called "Administrator" with no privileges, and a 10+ digit password that contains letters, numbers and non-alphanumeric characters, making it next to impossible to guess or crack. Enable log on Auditing so that you will know if somebody tries to access the account. To enable Auditing, go to Local Security Policy, and under Local Policies, select Audit Policy. In the right pane, open the setting Audit Logon Events and check both the Success and Failure boxes. You can review the Audit in Event Viewer (**Start > Run > eventvwr.msc**)

❍ When logging on by pressing [**Ctrl**] + [**Alt**] + [**Del**], the login window will display the name of the last user logged in. For hackers, this is sufficient information to start cracking the user account. You can disable the display of the last logged-in username from Local Security Policy (**Control Panel > Administrative Tools**). Select Security Options under Local Policies in the left pane. In the right pane, find the setting "Do not display last username in logonscreen" and change the value to Enabled.

❍ Encrypt your important files and folders with EFS (Encryption File System). Encrypting your files and folders will prevent hackers from reading encrypted data if they steal your hard disk, mount it on another system and take ownership of all the files and folders.



Encrypt Sensitive Folders

The encrypted files will not be accessible without the original logon credentials. When encrypting, ensure that you encrypt the entire folder and not just the files. If a folder is encrypted, any files created, moved or copied into the folder will also automatically be encrypted.

To encrypt a folder or file, right-click on it, select Properties, click on Advanced in the General Tab, and check "Encrypt contents to secure data".

9.1.3 Wi-Fi public hotspot security

While it may be cool to surf the Web from a Wi-Fi hotspot, you leave yourself exposed to hacker attacks if you do not secure your Wi-Fi access. Follow these steps to ensure a safe and secure wireless surfing experience from public hotspots.

❍ Ensure you are using a legitimate access point. As public hotspots become more common, hackers are setting up access points close to standard public hotspots with a similar SSID (Wireless Network Name). These connect directly to hacker databases that collect the usernames and passwords you use to log in. They can also collect credit card information if you use the public hotspot to make credit card payments. Verify the correct SSID name that you can connect to from a public hotspot. Do not set your laptop to automatically connect to any available Wi-Fi network. Turn off ad-hoc mode, which allows other Wi-Fi computers

to connect to yours, and when you are done surfing, turn off the Wi-Fi card.

❍ Set your Wi-Fi connection to use WPA or WEP encryption if the hotspot supports it. If the hotspot access point does not support encryption, all your data is being transmitted in clear text and can be easily intercepted by hackers. While data to HTTPS sites will be encrypted and relatively secure, regular e-mail and other traffic can still be read. Password-lock sensitive attachments and inform the recipient of the password by other means (phone, SMS, pre-agreed, or any other means you can think of).

❍ Use a personal firewall to prevent hackers from probing your system for open ports.

❍ Use an anti-virus solution to protect your laptop from virus attacks.

❍ Verify the overall security of your system by using Microsoft Baseline Security Analyzer.
❍ Test the overall security of your system by running the free tests at Gibson Research (**https://www.grc.com/x/ne.dll?bh0bkyd2**)

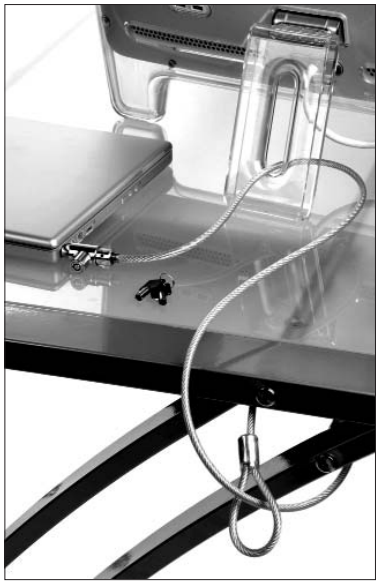
❍ When sending and receiving e-mail, don't use an e-mail client like Outlook, Thunderbird, Outlook Express, etc. Use Web-based e-mail that supports SSL or HTTPS. This will ensure that all mail data is encrypted between your laptop and the mail server.

❍ Be aware of people around you. Somebody may be looking over your shoulder and noting down any information you are typing. This may sound a bit extreme, but most identity thieves snoop around public places. Remember Andy Grover: "Only the paranoid survive!"

9.1.4. Security accessories

❍ Use a cable and lock to secure your laptop. Most laptops come with the Universal Security Slot for this purpose. Use a good qual-

ity cable and a tubular lock design rather than the regular tumbler lock. When chaining the laptop make, sure you are tethering it to a strong, immovable, unbreakable object. Just the presence of this in plain sight will deter many casual thieves.


Laptop cable and lock.jpg

❍ Use a biometric fingerprint scanner as your primary logon method. This will effectively lock out everybody except yourself from the machine.

❍ Unbelievable as it may sound, a significant portion of laptop theft happens in offices! Poorly-screened housekeeping staff, contractors and disgruntled employees are usually to blame. Protect your laptop from in-house theft by using a docking station that is fixed to your desk and which will lock the laptop in place if you plan to leave it in the office overnight.

9.2. Protecting Your Cell Phone

Next to laptops, cell phones and PDAs are the most vulnerable to theft. Secure your mobile devices using the following steps.

9.2.1. Phone/SIM Locks

Most modern cell phones offer multiple levels of code locks similar to the password in PCs. While it may be inconvenient, you should seriously consider code-locking your phone, especially if you are on the move for an extended period of time.

The first, of course, is the SIM card PIN Code. You will normally be given a PIN code when you purchase your SIM card. Actually you will be given four sets of codes when you purchase the phone: PIN1, PIN2, PUK1, and PUK2.

❍ PIN1 activates your phone when you first switch it on.

❍ PIN2 is used when you need to access some advanced functions.

❍ PUK1 is used if you forget or enter the wrong PIN1 code. If you enter the wrong PIN1 code three times, the SIM card locks and you will need to enter the PUK1 code to unlock it and reset your PIN1 code. If you lose your PUK number, there is no other recourse than to get a new SIM card from your cell phone service provider.

❍ PUK2 is similar to PUK1, and is used for PIN2.

Along with the above, you should also consider locking your phone with a phone-specific security code. This will effectively stop anyone from accessing the phone if they do not know the code. Even if they switch off the phone, remove the SIM and replace it with another, they will still be unable to access the phone without the security code.

One other measure is to use a keyguard code for locking your phone. Most cell phones support automatic locking of the keypad after a period of inactivity. This prevents dialling if the keys get inadvertently depressed when in your pocket. You will have to press a combination of keys (Nokia: Menu *) to unlock the phone or to manually lock it. You can set your phone to require a code when you unlock your keypad. Also make it a habit to manually lock your phone immediately after a call. Sometimes, the keyguard will fail to kick in as some key has already been accidentally depressed before the keyguard activation time-out.

In a scenario where a thief steals your phone and tries to make a call, the keyguard code will block access on an already-powered on phone. On restarting, the PIN request for the SIM will thwart him. If the SIM is changed, the phone's security code will also block access. The phone will become practically useless to the thief. You can rest assured that all your personal data will be protected, even though you may not be to recover it! Also, the thief could attempt to reset the security code by calling the cell phone vendor's customer service and pretending to be the owner. To prevent that, inform them of the theft as well as your mobile phone's IMEI number.

IMEI is short for International Mobile Equipment Identity. Every mobile device in the world has a unique number. The IMEI number will be usually found under the battery slab, Many phones will also display the IMEI number if you key in ***#06#**. Of course, you will need to take this precaution beforehand and store the IMEI number in a safe place—*not* on your cell phone, and not in your wallet!

If you have a Nokia phone, forgotten your security code, and have the IMEI number, you can go to **http://nfader.z-host.ru/** and generate a master security code using your phone IMEI number. You can use the master security code to override your personal security code and gain access to your mobile. You can then reset the security code as required.

9.3 Bluetooth Hacking

Bluetooth is great. You can snap pictures, take video clips with your camera phone, transfer it to your laptop, or beam it across to a friend's mobile. However, if you do not secure Bluetooth access on your phone, it is easily "discoverable" by other Bluetooth devices in the immediate vicinity. A person with a Bluetooth-enabled device can send you unsolicited messages, transfer viruses and worms to your phone, or even gain access and steal your personal data and / or corrupt it. An experienced Bluetooth hack-

er can gain access to your mobile phone commands, using it to make phone calls, send expensive international SMS messages, write entries into your phonebook, eavesdrop on your conversations, and even gain access to the Internet.

Bluetooth criminals are known to roam neighbourhoods with powerful Bluetooth detectors that search for Bluetooth enabled cell phones, PDAs, and laptops. They are known to fit laptops with powerful antennas that can pick up Bluetooth devices from within a range of 800 metres! The latest tactic is to force Bluetooth devices in hidden mode to pair with the attacker's device. This, however, is very labour-intensive, and is most often used against known targets who have large bank accounts or expensive secrets.

9.3.1 How it works

Almost all cases of Bluetooth attacks are a result of improper setup of the Bluetooth device. In most cases, Bluetooth devices are configured at security level 1, where there is no encryption or authentication. This enables the attacker to request information from the device that will be helpful in stealing it.

Once stolen, not only is the data on the device compromised, it will also compromise the data on all devices trusted by it. This can then be used to eavesdrop on conversations between other devices.

Additionally, Bluetooth uses the Service Discovery Protocol (SDP) to determine what services are offered by what devices in range. Attackers can use this information to launch service-specific attacks on any of the devices.

If the attacker is able to obtain the link keys and the addressing of two communicating devices, he can launch a man-in-the-middle type of attack where all information is routed through the attacker's device.

Attackers can also eavesdrop on devices that are pairing up for the first time. This will give the attacker sufficient information to

use an algorithm to guess the security key and pretend to be the other device.

9.3.2 Avoiding It

Securing your Bluetooth phone is easy. Take these few simple steps to ensure that your device is protected from Bluetooth attacks.

❍ Switch off Bluetooth when you are not using it. This will prevent unauthorised access for the most part. Only enable Bluetooth when you are actively transferring data from or to another device.

❍ Use a strong PIN code, one that is at least six to eight digits or longer.

❍ Many devices offer tons of features to maximise the usability of your Bluetooth connections. Review the documentation and disable all that are a security risk, and pay special attention to the security settings. Use encryption by default and only disable it if the device you are communicating with doesn't support it.

❍ Ensure that Bluetooth is running in hidden mode. When you are pairing it with another device, like a headset, you will need to run it in discoverable mode. Do this in a secure location like inside your office or home. Once the link has been established, go back to hidden mode. If for some reason the pairing breaks when in a public place, wait till you are in a secure location before re-pairing the two devices.

❍ Be aware of where you are. If you are in an open, public place, it is best to disable Bluetooth. Public wireless hotspots are a favourite hangout of "Bluejackers".

Further Resources

There is no such thing as "enough security"—be it with forts or padlocks or computers. Just when you think you have it all secured, a new threat looms in the background. This book has covered most aspects of security for a home PC. But there's so much more we could write about security, it would run into several books. Here, we present some Web links and book titles that you can use to further enhance your knowledge about computer security.

In many parts of this book, we have explained how the Internet is a source of viruses, worms and so on. Thankfully, there are many security sites that provide you with updates on new infections and the means to contain them. You can also become a member of a security forum and learn from the discussions there. This apart, certain books also can help you in understanding issues relating to security.

10.1 Online Resources

Let us first take a look at some Web sites that can help you know what's happening in the world of security and what action you can take when something comes up on that front.

Microsoft Security Updates

www.microsoft.com/security

This site has security updates as well as tools and tips. Here, you can find security updates for any Microsoft products

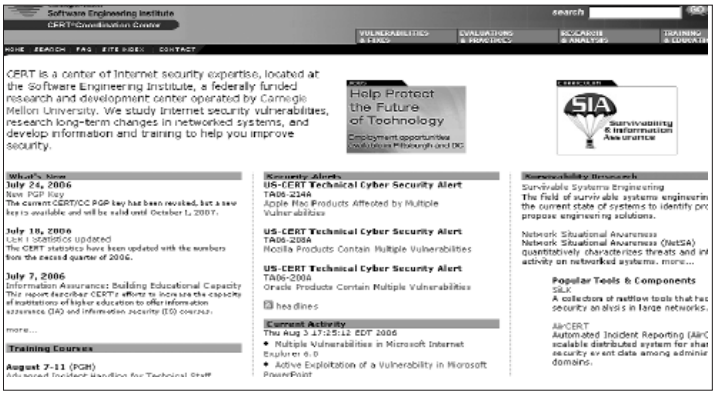
you may be using. On the left side of the page, you will find links that take you to different sections such as information for home security, news for IT professionals, and much more. When you click on "Home Users", for instance, you will be taken to a page that has information and tips pertaining to home security.

CERT

www.cert.org

CERT is a project maintained by Carnegie Mellon University to study Internet security vulnerabilities, research long-term changes in networked systems, and develop information to improve IT security. Look for two sections called "Security Alerts" and "Current Activity", which provide information on security threats and particular trends. Most of the news here is aimed at people at the level of system administrator, but some of them it can be used by home users as well. If you wish to know what's happening in IT security, this is a good site to visit. There are even statistics pertaining to virus / worm infections and vulnerabilities.

CERT has separate Web sites and working teams for different geographic areas, including India.



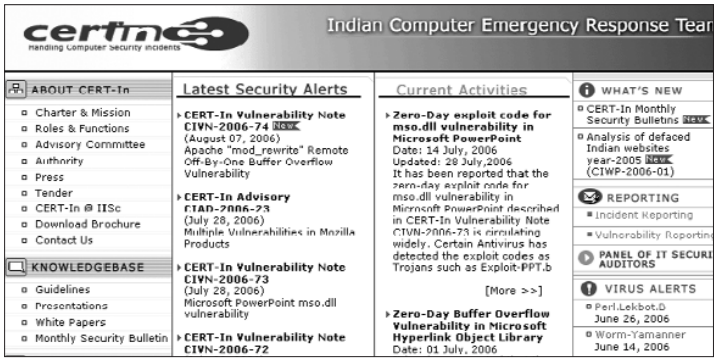
NASSCOM

www.nasscom.in

The Web site of NASSCOM (National Association of Software and Services Companies) contains information on several aspects of IT and outsourcing in the Indian context. There is a section dedicated to security and cyber offences under the "Resource Center" link. Click on "Be-Secure Newsline" under the Resource Center link on the homepage. There isn't a whole lot of content, but it's got to do with the scenario in India.

CERT-In

www.cert-in.org.in



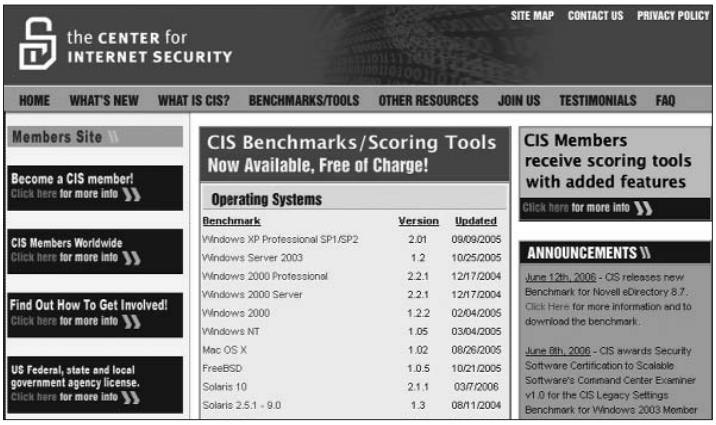
CERT-IN is the Indian Computer Emergency Response Team, which is meant to respond to computer security incidents as and when they occur. CERT-In operates with authority delegated by the Department of Information Technology, and the Ministry of Communications and Information Technology of the Government of India. It also aims to assist members of the Indian IT community in implementing proactive measures to reduce the risks of computer security incidents. The site features white papers and presentations apart from security alerts. Clicking on the link to the left called "Vulnerability Notes" takes you to a list of vulnerabilities ordered by date.

The "Press" link takes you to a section that contains news released to the media by CERT-In.

Center for Internet Security

www.cisecurity.org

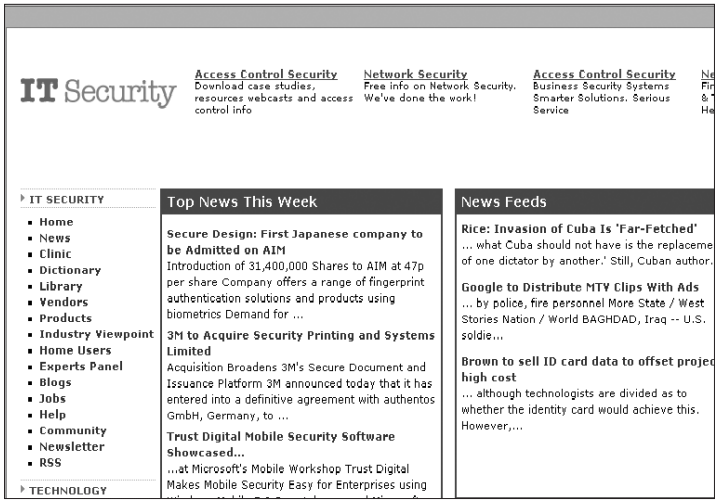
The Center for Internet Security (CIS) is a non-profit enterprise whose mission is to help organisations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. This site, again, is meant for system administrators in a business, but if you are interested in security issues, you can pick up some information here. Part of the focus of this Web site



is the security benchmarking tool, which can be downloaded free of cost to test the security policies in a network or even a home system.

Under the link called "Other Resources", you'll find several articles in PDF format, but these largely pertain to the US governmental laws on IT security—just in case you're interested.

ITsecurity.com
www.itsecurity.com



This is an all-in-one Web site that features information for both home users as well as system or network administrators. The site features a dictionary of security terms, a blog, a library that contains articles and white papers, security hardware vendor information, and more. You can also subscribe to a newsletter.

Secunia
http://secunia.com

Secunia is a Danish computer security service provider. They are best known for tracking vulnerabilities in software and operating systems. Secunia, on its site, says it monitors vulnerabilities in

software such as Internet Explorer, Firefox, Opera, and... the list of software and operating systems in the Secunia database currently includes 11,361 items! If you use a certain software, in all probability, you will find it in Secunia's database.

Information is added to the database daily, through software suggestions from customers and vulnerability reports affecting new software.

You'll need to check out the page to see the sheer amount of useful information there. And most of what you need to know is right there on the index page - highlights, and the latest advisories. The “highlights” section is usually one of the first places on the Web where critical security information crops up on the Web.

Sophos

www.sophos.com

Sophos is a security firm that makes anti-virus software and such. But their Web site holds more than just information about their products - the latest security threats are listed, as are the latest “news, events and awards.” There's a “hot topic” on the index page,

where you can get in-depth information on a topic; there's also a "have your say" section. If you're really paranoid, you can subscribe to an RSS feed that delivers the latest security-related news and developments.

Kaspersky Lab

www.kaspersky.com

The "viruslist" on this site calls itself the "largest encyclopedia of malware." There's a "virus watch" section, where, like at

some of the other sites we've mentioned, you can find a list of the latest viruses. Another must-visit for those concerned about security, partly because at Kaspersky Linux Security, you can find anti-virus and anti-spam products for protecting your Linux systems.

SecurityFocus

www.securityfocus.com

SecurityFocus is probably the most comprehensive and trusted source of security information on the Internet. It is a vendor-neutral site that provides objective, timely and comprehensive security information to "all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs."

Here is another site you'll have to look at to get an idea of how much information is available out there. The index page features news, columnists, newest vulnerabilities, a search bar, the latest security-related incidents, and much more. You can subscribe to newsletters as well.

10.2 Online Virus / Trojan Scans

All viruses are bad. Some are worse, and can render your anti-virus software useless. Let's say you haven't updated your anti-virus software, and a new virus that disables anti-virus programs strikes. It would not let you install another anti-virus either. This is where online virus scans come in handy. Many anti-virus makers have an online virus scan facility. In case of an emergency, you can use the following links:

Housecall
http://housecall.trendmicro.com
This service from Trend Micro is one of the oldest and most well-known online scanning services.

BitDefender
www.bitdefender.com/scan8/ie.html
From the site, "BitDefender Online Scanner is a fully-functional anti-virus product. It features all required elements for thorough anti-virus scanning and effective cleaning: it scans your system's memory, all files, folders and drives' boot sectors, providing you with the option to automatically clean the infected files."

PC-Pitstop
www.pcpitstop.com/antivirus/ AVLoad.asp
Pcpitstop.com offers a variety of tests besides an anti-virus scan—Internet speed, privacy scan, spyware scan, a "quick scan," "Exterminate", driver scan, disk health, and more.

Jotti.org
http://virusscan.jotti.org
You can submit a file here for an anti-virus test. Useful if you've received a file from someone and you don't have an anti-virus (or one that's not updated.)

Windowsecurity.com
www.windowsecurity.com/trojanscan

This is an online Trojan scanning service. It needs IE 5 or above with ActiveX enabled.

McAfee
http://us.mcafee.com/root/mfs/ default.asp
This is an online anti virus scanning service from well-known anti-virus maker McAfee.

10.3 Forums

Online forums exist on almost every topic conceivable, security included. To know from people who are more experienced than

Subject	Posted By	Time & Date	Replies
Virus or computer issue??	sykadelik	06:27:56 8/07/06	(0)
someone plz PLZ help me!	takeshi	22:59:24 8/06/06	(0)
Anti Virus	stuffie999	20:39:05 8/06/06	(1)
Fire wall is blocking programs	boddah1	06:59:11 8/07/06	(5)
Trojan Factory is kicking my....	Rankin	18:00:09 8/06/06	(4)
Suspected Problem with Explorer	kotoro	15:50:12 8/06/06	(0)
Slow pc	Harry456	06:32:16 8/07/06	(3)
slow start up and randomly freezes	candiehearts	18:39:50 8/06/06	(6)
For All With Malware	jeremyofmany	15:25:36 8/06/06	(4)
Website Access crap	Hansuke	05:16:28 8/07/06	(2)
Need to remove iworm_attck_v122.02a	qsteph	19:59:50 8/06/06	(9)
NIS 2005 problem	pault2005	11:04:34 8/06/06	(4)
help please!	kmas	12:58:44	(31)

You can get help on almost any security-related issue at many forums entirely dedicated to the topic

you are, you can join a forum and observe what's going on. You can post your queries and have them answered—and gradually start replying to other's questions if you know the subject well enough. Don't post frivolous questions: you could end up irritating some people—watch the forum for a while to gauge the level of the discussions, and look at older threads as well. You will need to register to get access to topic threads in the forums.

Here are some links to forums that focus on security issues:

http://computing.net/security/wwwboard/wwwboard.html

www.security-forums.com

www.castlecops.com/c2-Security.html

http://forums.techguy.org/54-security

Notes

Notes

Notes

Notes

Notes