Hackers and Browser Hijacking is one area of the Net that affects everyone at some stage.

In addition to having third party utilities such as SpyBot, Anti Virus scanners and firewalls installed there are some changes that can be made to Windows 2000/XP. Below are some details to make your system safer from hackers and hijackers.

Some of these tips require editing of the Registry so it is wise to either backup the registry and/or create a Restore Point.

1. Clearing the Page File at Shutdown

Windows 2000/XP paging file (Sometimes called the Swap File) can contain sensitive information such as plaintext passwords. Someone capable of accessing your system could scan that file and find its information. You can force windows to clear out this file.

In the registry navigate to HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlSession ManagerMemory Management and add or edit the DWORD ClearPageFileAtShutdown. Set it to 1.

Note that when you do this, the system will take much longer to shut down: a system with a really big Page File (! Gig or more) may take a minute or two longer.

2. Disable the POSIX and OS/2 Subsystem.

Windows 2000 and XP come with little-documented subsystems it at allow compatibility with UNIX and OS/2 systems These rues systems are enabled by default but so rarely used that they are best off bring disabled completely to prevent possible service hijackings.

To disable these subsystems, open the registry and navigate to HKEY LOCAL MACHINESYSTEMCurrentControlSetControlSession ManagerSubSystems. Delete the subkeys Os2 and Posix. then reboot.

3. Never leave default passwords blank.

On installation, Windows 2000 sets up an Administrator account with total system access and prompts for a password. Guess what: by default, it allows that password to be blank. If a user doesn't want to type a password, he can simply click Next and the system will be an open door for anyone who wants to log on. Always opt for a password of some kind when setting up the default account on a machine.

4. Install Windows In a different directory.

Windows usually installs itself in the WINDOWS directory. Windows NT 4 0 and 2000 Will opt for WINNT. Many worms and other rogue programs assume this to be the case and attempt to exploit those folders files. To defeat this install Windows to another directory when you're setting it up - you can specify the name of the directory during setup. WINDIR is okay; so some people use WNDWS - A few (not that many) programs may not install properly if you install Windows to another folder but t hey are very few and they are far between

5. Fake out hackers with a dummy Administrator account

Since the default account in Windows 2000 is always named Administrator, an enterprising hacker can try to break into your system by attempting to guess the password on that account. It you never bothered to put a password on that account, say your prayers.

Rather than be a sucker to a hacker, put a password on the Administrator account it you haven't done so already. Then change the name of the Administrator account. You'll still be able to use the account under its new name, since Windows identifies user accounts by a back-end ID number rather than the name. Finally, create a new account named Administrator and disable it. This should frustrate any would -be break-ins.

You can add new accounts and change the names of existing accounts in Windows 2000 through the Local Users and Groups snap in. Right-click on My Computer, select Manager, open the Local Users and Groups subtree, look in the Users folder and right-click on any name to rename it. To add a new user, right-click on the containing folder and select New User. Finally, to disable an account, double-click it, check the Account is disabled box and click OK.

Don't ever delete the original Administrator account. Some programs refuse to install without it and you might have to log in under that account at some point to setup such software. The original Administrator account is configured with a security ID that must continue to be present in the system.

6. Disable the Guest account

Windows XP comes with a Guest account that's used for limited access, but it's still possible to do some damage with it. Disable it completely if you are not using it. Under Control Panel, select User Accounts, click on Guest Account and then select Turn Off the Guest Account.

7. Set the Hosts file to read-only to prevent name hijacking.

This one's from (and to a degree, for) the experts. The HOSTS file is a text file that all flavors of Windows use to hold certain network addresses that never change. When a network name and address is placed in HOSTS, the computer uses the address listed there for that network name rather than performing a lookup (which can take time). Experts edit this file to place their most commonly-visited sites into it, speeding things up considerably.

Unfortunately hijackers and hackers also love to put their own information into it - redirecting people from their favorite sites to places they don't want to go. One of the most common entries in HOSTS is local host which is set 1770.0.1. This refers to the local machine and if this entry is damaged the computer can behave very unpredictably.

To prevent HOSTS from being hijacked, set it to read-only. Go to the folder %Systemroot%system32driversetc, right-click on HOSTS, select Properties check the Read-Only box and click OK. If you want to add your own entries to HOSTS, you can unprotect it before doing so, but always remember to set it to read-only after you're done.

8. Disallow changes to IE settings through IE

This is another anti hijacker tip. IE can be set so that any changes to its settings must be performed through the Internet icon in the Control Panel, rather than through IE's own interface. Some particularly unscrupulous programs or sites try to tamper with setting by accessing the Tools, Options menu in IE. You can disable this and still make changes to IE's settings through the Control Panel.

Open the Registry and browse to HKEY_CURRENT_USER SoftwarePoliciesMicrosoftInternet ExplorerRestrictions. Create or edit a new DWORD value named NoBrowserUptions and set it to 1 (this is a per-user setting). Some third-party programs such as Spybot Search And Destroy allow you to toggle this setting.

You can also keep IE from having other programs rename its default startup page, another particularly annoying form of hijacking. Browse to HKEY.CURRENT USERSoftwarePolicies MicrosoftInternet ExploreControl Panel and add or edit a DWORD, Homepage and set it to 1.

9. Turn off unneeded Services

Windows 2000 and XP both come with many background services that don't need to he running most of the time: Alerter, Messenger, Server (If you're running a standalone machine with no file or printer shares), NetMeeting Remote Desktop Sharing, Remote Desktop Help Session Manager (the last two if you're not using Remote Desktop or NetMeeting), Remote Registry, Routing and Remote Access (if you're not using Remote Access), SSDP Discovery Service, Telnet, and Universal Plug and Play Device Host.

A good resource and instruction on which of these services can be disabled go to
/http://www.blkviper.com/WinXP/

10. Disable simple File Shares.

In Windows XP Professional, the Simple File Sharing mode is easily exploited, since it’s a little too easy to share out a file across your LAN (or the NET at large). To turn it off, go m My Computer, click Tools, Folder Option and the View tab, and uncheck Use Simple file sharing (Recommended). Click OK. When you do this you can access the Security tab in the Properties window for all folders; set permissions for folders; and take ownership of objects (but not in XP Home)