Basic Security Measures

Provide Physical Security for the machine

It may seem basic, but we didn't want you to overlook the obvious. The simple fact is that most security breaches in corporate environments occur from the inside. Keep your workstation in an office that locks, install a lock on the CPU case, keep it locked, and store the key safely away from the computer at a secure location. (i.e. a locked cabinet in the server room)

Use NTFS on all your partitions

The FAT16/FAT32 file systems that were shipped with Windows 95/98/ME offered no security for your data and left your system wide open to attacks. The NTFS file system is faster than FAT32 and allows you to set permissions down to the file level. If you're unsure of how your system is configured, open **My Computer**, right click on the drive letter you want to check, and select "**Properties**" from the menu. If your Windows XP system was preconfigued with the FAT16 or FAT32 file system, you can convert the partitions quickly and easily using the convert.exe utility. (If you choose to convert to NTFS, you cannot go back to the FAT or FAT32 file system unless you reinstall XP) In addition, using NTFS on Windows XP Professional allows you to encrypt files and folders using the Encrypting File System (EFS). If you are dual booting Windows XP and Windows 9x/Me, keep in mind that these operating systems cannot read NTFS partitions, and you won't be able to access the files when you are in Windows 9x/ME

Disable Simple File Sharing

Both Windows XP Home Edition and XP Professional workstations that are *not* part of a domain, use a network access model called "Simple File Sharing," where all attempts to log on to the computer from across the network are forced to use the Guest account (to prevent them from using a local Administrator account that wasn't configured with a password) This means that if you're connected to the internet and don't use a secure firewall, your files contained within those shares are available to just about anybody.

To disable Simple File Sharing on XP Professional:

- Click **Start > My Computer > Tools > Folder Options**
- Select the **View** tab
- Go to **Advanced Settings,**
- clear the Use **Simple File Sharing** box
- click **Apply**

Unfortunately, XP Home Edition doesn't allow you to disable Simple File Sharing and is unable to join a domain, so the best you can hope for is to make sure you set your shared folders to be read only, hide the file shares by using a $ sign after the folder name, or if your using the NTFS file system, use the 'Make Private" option in the folder properties. Windows XP Professional workstations that are part of a domain or that have Simple File Sharing disabled, use the "Classic" NT security model that requires all users to authenticate before granting access to shared folders. For more information on File Sharing in XP, see KB Article 304040.

Use passwords on all user accounts

Both Windows XP Professional and Home Edition allow user accounts to utilize blank passwords to log into their local workstations, although in XP Professional, accounts with blank passwords can no longer be used to log on to the computer remotely over the network. Obviously, blank passwords are a bad idea if you care about security. Make sure you assign passwords to all accounts, *especially* the Administrator account and any accounts with Administrator privileges. By the way, in XP Home Edition **all** user accounts have administrative privileges and no password **by default**. Make sure you close this hole as soon as possible

Use the Administrator Group with care

It's very common for home users and small business administrators to simply give all local accounts full Administrator privileges in order eliminate the inconvenience of logging into another account. However this practice gives a hacker the opportunity to try to crack a greater number of administrator level accounts and increases his/her chance for success. It also increases the odds that malicious code executed via an e-mail attachment or other vector can do more damage to your

files. In a workgroup consider placing local users with a greater need for control in the local Power Users group, instead of the Administrators group. And avoid the temptation of using the local administrator account as your default login account.

Disable the Guest Account

The guest account has always been a huge hacker hole, and should be disabled as soon as you install your workstation. Unfortunately, this setting recommendation only applies to Windows XP Professional computers that belong to a domain, or to computers that do not use the Simple File Sharing model. *Windows XP Home Edition will not allow you to disable the Guest account. When you disable the Guest account in Windows XP Home Edition via the Control Panel, it only removes the listing of the Guest account from the Fast User Switching Welcome screen, and the Log-On Local right. The network credentials will remain intact and guest users will still be able to connect to shared resources of the affected machine across a network. Microsoft Knowledge Base Article: 300489 describes this behavior and states that it is by design. The best workaround for XP Home Users is to assign a strong password to the Guest account.*

Use a firewall if you have a full time internet connection

Having instant, high speed access to the internet is a real convenience but it also puts your data at risk. Although XP comes with a built in firewall (called ICF), it is not enabled by default, and it only filters incoming traffic without attempting to manage or restrict outbound connections at all. While this may be fine for most users, we highly recommend using a third party personal firewall such as BlackIce if you're concerned about your data. For corporate users already behind a firewall, consider using Group Policy to enable ICF and disable specific ports when users are not connected to the corporate network. For more information on ICF, see: HOW TO: Enable or Disable Internet Connection Firewall in Windows XP (Q283673)

Use a router instead of ICS

The Internet Connection Sharing feature within XP allows a user to connect one PC to the internet and then share that connection with the rest of the computers within his home or small office network. While it was generally a good idea when it was conceived, if you have a high speed connection a real router is a faster, easier to configure, and more secure. For small home or office, we strongly recommended the Linksys Cable/DSL Routers, which are usually under $100.00.

Install AntiVirus Software on all workstations

Viruses and other forms of malicious software have been around for years, but today's malware utilizes the internet and e-mail systems to spread globally in a matter of hours. Installing AntiVirus software is a basic step in protecting your data, but it's near useless if the definitions aren't updated.

Keep up to date with hotfixes and service packs

Windows XP is a complex operating system and is not immune to its own bugs and security holes. Its common tactic for hackers to use the latest known security hole to break into a system and work backward from there until they find an open door that gives them full access. In fact 99% of system breaches are executed using known security vulnerabilities that were never patched. Use the Windows Update feature or automatic update to keep your system up to date. You can also use the Microsoft Baseline Security Analyzer to check your system for known vulnerabilities.

To enable automatic update in Windows XP:

- Click **Start**, click **Control Panel**, click **Performance and Maintenance**, and then click **System**.
- On the **Automatic Updates** tab, click the setting of your choice

Password protect the screensaver

Once again this is a basic security step that is often circumvented by users. Make sure all of your workstations have this feature enabled to prevent an internal threat from taking advantage of an unlocked console. For best results, choose the blank screensaver or logon screensaver. Avoid the OpenGL and graphic intensive program that eat CPU cycles and memory. Make sure the wait setting is appropriate for your business. If you can get your users in the habit of manually locking their workstations when they walk away from their desks, you can probably get away with an idle time of 15 minutes or more. You can keep users from changing this setting via Group Policy or the local security policy.

Secure your wireless network
The new 802.11 wireless standard allows you to roam freely without cables and make anywhere your virtual office. This also gives hackers another open door to your data if you fail to lock it. A recent survey in the U.K found that of 5,000 wireless networks that were discovered by simply driving around the city with a wireless enabled laptop, 92% were wide open. As "drive by" hacking and warchalking are becoming common practice, any hacker with a laptop and a Pringles can could potentially compromise your network. We could go into a whole new checklist on securing your wireless network but KB Article Q309369 is a good place to start.

Secure your Backup tapes
It's amazing how many organizations implement excellent platform security, and then don't encrypt and/or lock up their backup tapes containing the same data. It's also a good idea to keep your Emergency Repair Disks locked up and stored away from your workstations as well.

Intermediate Security Measures

Use the Security Configuration Manager and templates provided with XP Professional
The Security Configuration Manager (SCM) set of tools allows security administrators to define security templates that can be applied to individual machines or any number of machines via group policy. Security templates can contain password policies, lockout policies, Kerberos policies, audit policies, event log settings, registry values, service startup modes, service permissions, user rights, group membership restrictions, registry permissions and file system permissions. Microsoft provides a number of predefined security templates to help you lock down your PC via Group Policy. These templates represent low, medium, and high security configurations, which can be customized to meet your specific security needs. The security relevant registry values configurable by SCM appear under Local Policies\Security Options when using SCM tools such as the security templates snap-in, the security configuration and analysis snap-in, or the security settings extension to Group Policy. *Note: This feature is not available on Windows XP Home Edition*

Password Security
A good password policy is essential to your network security, but is often overlooked. In large organizations there is a huge temptation for lazy administrators to create all local Administrator accounts (or worse, a common domain level administrator account) that uses a variation of the company name, computer name, or advertising tag line. i.e. *%companyname%*#1, win2k*%companyname%,* etc. Even worse are new user accounts with simple passwords such as "welcome", "letmein", "new2you", that aren't required to changed the password after the first logon. Use complex passwords that are changed at least every 60 -90 days. Use Group Policy or the local computer policy to set restriction on password age, length, complexity, lockout duration, and number of bad attempts. (Click **Start** > **Run** > type **GPEDIT.MSC** > Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policy** > **Security Options**) Passwords should contain at least eight characters, and preferably nine (recent security information reports that many cracking programs are using the eight character standard as a starting point). Also, each password must follow the standards set for strong passwords. The basic goal is that the password should be complex enough to foil hacker attempts, and not so complex that users will have difficulty remembering their passwords and end up writing them on sticky notes pasted to the bottom of their keyboards.

Use software restriction policies
Using a software restriction policy, you can prevent unwanted programs from running; this includes viruses and Trojan horses, or other software that is known to cause conflicts when installed. Software restriction policies can also be used on a standalone computer by configuring the local security policy, or can integrate with Group Policy and Active Directory. (Click **Start** > **Run** > type **GPEDIT.MSC** > Go to **Computer Configuration** > **Windows Settings** > **Security Settings** >**Software Restriction Policies**)
Note: This feature is not available on Windows XP Home Edition

Limit the number of unnecessary accounts
Eliminate any duplicate user accounts, test accounts, shared accounts, general department accounts, etc., Use group policies to assign permissions as needed, and audit your accounts

regularly. These generic accounts are famous for having weak passwords (and lots of access) and are at the top of every hacker's list of accounts to crack first. This can be a big problem at larger companies with understaffed IT departments. An audit at a Fortune 10 company I worked for revealed that 3,000 of their 15,000 active user accounts were assigned to employees who no longer worked for the company. To make matters worse, we were able to crack the passwords on more than half of those inactive accounts.

Rename the Administrator Account

Many hackers will argue that this won't stop them, because they will use the SID to find the name of the account and hack that. Our view is, why make it easy for them. Renaming the Administrator account will stop some amateur hackers cold, and will annoy the more determined ones. Remember that hackers won't know what the inherit or group permissions are for an account, so they'll try to hack any local account they find and then try to hack other accounts as they go to improve their access. If you rename the account, try not to use the word 'Admin" in its name. Pick something that won't sound like it has rights to anything.

Consider creating a dummy Administrator account

Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +10 digit complex password. This should keep the script kiddies busy for a while. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with.

Replace the "Everyone" Group with "Authenticated Users" on file shares

"Everyone" in the context of Windows XP security, means anyone who gains access to your network can access the data. Never assign the "Everyone" Group to have access to a file share on your network, use "Authenticated Users" instead. This is especially important for printers, who have the "Everyone" Group assigned by default.

Prevent the last logged-in user name from being displayed

When you press Ctrl-Alt-Del, a login dialog box appears which displays the name of the last user who logged in to the computer, and makes it easier to discover a user name that can later be used in a password-guessing attack. This can be disabled via the Group Policy snap in. (Click **Start** > **Run** > type **GPEDIT.MSC** > Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policy** > **Security Options**)

Make sure that Remote Desktop is disabled

Remote Desktop is a new feature in Windows XP Professional that allows you to connect to your computer remotely and work as though you are sitting at the console. While this may be convenient for some users, it also makes it easier for a hacker who has compromised one of your user accounts to log in directly to your machine from a remote location. Fortunately, remote desktop is not enabled by default on Windows XP Professional, and is not available for Windows XP Home Edition. For more information see KB Article Q306300

You can make sure it stays off your PC's on your network by using Group Policy.

To use the computer's local group policy to disable Remote Desktop:

1. Click **Start**, click **Run**, type **gpedit.msc**, and then click **OK**.
2. In the Group Policy editor, click to expand **Computer Configuration**, click to expand **Administrative Templates**, click to expand **Windows Components**, and then click to expand **Terminal Services**.
3. Double-click the **Do not allow new client connections policy.**
4. **Set the policy to Enabled, and then click OK.**

You can also use the following procedure to disable Remote Desktop; however, if you use the preceding procedure, the following configuration is overridden:

1. **Right-click My Computer and click Properties.**
2. **Click the Remote tab.**
3. **In the Remote Desktop section, click to clear Allow users to connect**

remotely to this computer, and then click OK.

***NOTE**: Remote Desktop is not available in Windows XP Home Edition*

Disable unnecessary services

An unnecessary service is an unnecessary hacker hole, as well as a drain on system resources. You can disable services via **Control Panel > Administrative Tools > Services**

You may wish to consider disabling the following services:

- **Disable IIS** - Luckily, IIS in not installed by default in Windows XP. If you enabled it during your installation, and aren't using it you should disable it. If you are using IIS on your workstation, you need to take extra precautions to lock it down and stay on top of security vulnerabilities specific to web services.
- **Netmeeting Remote Desktop Sharing**
- **Remote Desktop Help Session Manager -** If you haven't disabled this via Group Policy already
- **Remote Registry**
- **Routing & Remote Access** - if your not dialing into your machine.
- **SSDP Discovery Service** - this disables the Universal PNP Service, which leaves TCP Port 5000 wide open.
- **Universal Plug and Play Device Host -** This is designed to allow your computer to automatically connect to network-enabled appliances. Although there are no practical uses for this technology yet, several severe security flaws have already been discovered. Use the UnPlug and Pray utility from Gibson Research to disable "Universal Plug and Play". Gibson's web site has additional information about why this is necessary
- **Telnet**

Enable EFS (Encrypting File System)

Windows XP Professional ships with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing your files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on Folders, not just files. All files that are placed in that folder will be encrypted. For more information check out our EFS Resource Center *Note: This feature is not available on Windows XP Home Edition*

If you use Offline Folders, encrypt the local cache

With Windows XP, you can mark any shared folder that is available on the network (or any Web page) to be made available offline. The contents of these shared folders (or pages) are copied to an Offline Files database that is known as the client-side cache, where you can access them when not connected to the network. To safeguard offline files against theft, you can specify that the client-side cache is encrypted. To encrypt the Offline Files database on a local computer: Click **Start** >**Folder Options** > select the **Offline Files** tab > If Offline Files are not already enabled, click the **Enable Offline Files** option > Click the **Encrypt offline files to secure data** option > Click **OK**. *Note: When encryption of offline files is enabled or disabled, the entire database is affected; you cannot encrypt only some offline files. Also, if you are using the Fast User Switching feature in Windows XP, you will not be able to use offline files, and none of the options on the **Offline Files** tab will be available. To disable Fast User Switching, use the User Accounts utility in Control Panel.*

Encrypt the Temp Folder

Applications such as Microsoft Office use the temp folder to store copies of files while they are being updated or modified, but they don't always clean the folder when you close the program. Encrypting the temp folder provides an extra layer of security for your files. *Note: This feature is not available on Windows XP Home Edition*

Clear the page file at shutdown
The Windows XP Page file can occasionally contain passwords and other sensitive data that your system has stored into memory. You can force the operating system to clear the page file by using the Local Computer Policy via the MMC, or via Group Policy

---

Advanced Security Settings

Enable Auditing on your Workstations
While this is a fairly normal practice for servers, it isn't usually performed on workstations unless there is a high risk of data theft. Our philosophy is that the time to fix the roof is before it starts to rain. By selectively auditing a few key actions, you'll have a place to start investigating theft or destruction of data if someone ever does compromise your workstation. We recommend auditing the following actions:

Event	Level of Auditing
Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Success
Policy change	Success, failure
Privilege use	Success, failure
System events	Success, failure

For more information see KB article Q310399

Disable default shares
Windows XP automatically creates a number hidden administrative shares that the operating system uses to manage the computer environment on the network. These default shares can be disabled via the Computer Management console in the Control Panel, but they are re-enabled by the system after you restart your computer. The default hidden shares are:

Path and Function	
C$ D$ E$	Root of each partition. For a Windows XP Professional computer, only members of the Administrators or Backup Operators group can connect to these shared folders.
ADMIN$	%SYSTEMROOT% This share is used by the system during remote administration of a computer. The path of this resource is always the path to the Windows XP system root (the directory in which Windows XP is installed: for example, C:\Winnt).
FAX$	This used by fax clients in the process of sending a fax. The shared folder temporarily caches files and accesses cover pages stored on the server.
IPC$	Temporary connections between servers using named pipes essential for communication between programs. It is used during remote administration of a computer and when viewing a computer's shared resources
NetLogon	This is used by the Netlogon service to process log on requests
PRINT$	%SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS Used during remote administration of printers.

To prevent these shares from being created at startup, open RegEdit and edit the following key: **HKeyLocal Machine\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters** Create a DWORD value called AutoShareWks and set the parameter to 0. (Note: This does not disable the IPC$ share in our tests, we're still working on a solution). You should test the functionality of your programs and services after you disable the default administrative shares. Some Windows services depend on the existence of these shares. In addition, some third-party programs may require that some of the administrative shares exist. For example, some backup programs may require these shares. You may be able to restore functionality by manually creating the required shares.

Disable Dump File Creation

A dump file can be a useful troubleshooting tool when either the system or application crashes and causes the infamous "Blue Screen of Death". However, they also can provide a hacker with potentially sensitive information such as application passwords. You can disable the dump file by going to the **Control Panel > System > Advanced > Startup and Recovery** and change the options for 'Write Debugging Information" to None. If you need to troubleshoot unexplained crashes at a later date, you can re-enable this option until the issue is resolved but be sure to disable it again later and delete any stored dump files

Disable the ability to boot from a floppy or CD ROM on physically unsecured systems.

There are a number of 3rd party utilities that pose a security risk if used via a boot disk (including resetting the local administrator password.) If your security needs are more extreme, consider removing the floppy and CD drives entirely. As an alternative, store the CPU in a locked external case that still provides adequate ventilation. You can also restrict access to the floppy and CD-ROM drives in Windows XP Professional via the Local Computer Policy in the MMC (Click **Start** > **Run** > type **GPEDIT.MSC** > Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policy** > **Security Options**)

Disable AutoRun for the CD-ROM

One of the easiest ways for a hacker with physical access to a company's PC's to distribute malicious code is via the CD-ROM. By creating a custom CD with a payload set to launch from the autorun feature in any machine, a hacker can affect any number of unlocked systems without ever leaving a fingerprint or touching a keyboard. Or he/she can simply leave a few of these lying around the office marked "MP3's", or "Payroll Data" and wait for an unsuspecting user to simply pick it up and insert it into their machine. You can disable this function in Windows XP Professional by clicking **Start** > **Run >** and type **GPEDIT.MSC** Then go to **Computer Configuration** > **Administrative Templates** > **System** > Locate the entry for**Turn autoplay off**

Consider using SmartCard or Biometric devices instead of passwords.

The more stringent your password policy is, the more likely your users will begin keeping paper password lists in their desk drawers, or taped to the bottom of their keyboard. Windows 2000 supports these devices, so consider the costs vs. risks of your most sensitive data. When using smart cards please make sure to apply configure your workstation to lock if you remove the smart card. Under **Local Policies** > **Security Options** > **Interactive logon** > **Smart card removal behavior** >**Lock Workstation setting**

Consider implementing IPSec

Basically, IPSec provides encryption for network sessions using the Internet Protocol (IP) and promises to offer transparent and automatic encryption of network connections. For more information, click here