

Rid your XP computer of viruses/spyware and increase it's speed:

By: Dan Martin

This is by no means an example of everything that can or should be done to speed up an XP system or to get rid of Viruses, Trojans, Spyware or the like. If you have specific things that you do that are as good or better, I'm all for hearing about it. I would like this to be an evolving document designed for any technician so that they could reference this when having to deal with this type of problem.

**** NOTE:**** This document is an "at your discretion" document. It is not intended for use in any school system, corporation, business, or etc. It is solely for your use should you choose to do so. The author is in no way responsible for any use of any process, program, or idea given or implied.

Use a **CD** with the following files:

- Hijackthis
http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis/download
- AVG Anti-virus (Free)
<http://free.grisoft.com/doc/downloads?prd=aff>
- AVGS Anti-spyware
<http://free.grisoft.com/doc/downloads-products/us/frt/0?prd=asf>
- Spybot SD
<http://www.safer-networking.org/en/mirrors/index.html>
- Decrapifier
- PC Tools Firewall Plus
http://www.pctools.com/firewall/?ref=google_free&gclid=CICfkrLz0JECFQJJsgodhSzd2g
- Regclean
<http://www.majorgeeks.com/download458.html>

Start (boot) the system in "Safe Mode"

1. Turn off "System Restore"

Manual steps to turn off or turn on System Restore

Steps to turn off System Restore

Click **Start**, right-click **My Computer**, and then click **Properties**.

In the System Properties dialog box, click the **System Restore** tab.

Click to select the **Turn off System Restore** check box. Or, click to select the **Turn off System Restore on all drives** check box.

Click **OK**.

When you receive the following message, click **Yes** to confirm that you want to turn off System Restore:

You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your computer.

Do you want to turn off System Restore?

After a few moments, the **System Properties** dialog box closes.

2. If another antivirus is installed, remove it. (be sure you are NOT connected to the internet at this time.)
3. Install AVG Antivirus - If it was already installed, remove it and re-install to get a clean install. You will need to shut down between uninstall and re-install. Be sure to come back in "Safe Mode" again. Again... do NOT be connected to the Internet at this time.
4. Scan the system for viruses. Clean the virus if possible. Quarantine if needed. Delete only as a last resort.
5. Install AVG Antispyware and scan. Same procedure except you should just go by the "recommended" actions in AVGS.
6. Use "Hijackthis" to test for other problems in the registry. Make a backup of the registry first before doing any changes.
7. Use "Decrapifier" to get rid of extraneous applications that muddle the system down to a crawl.
8. Make sure that the IP is set to DHCP and that IE is set to automatically detect settings. (In IE, go to "Tools," "Internet Options," "Connections" tab, "LAN Settings" button, and make sure the "Automatically detect settings" check box is checked.)
9. Install Spybot SD as a second anti-spyware software package.
10. Set AVG and AVGS to auto-run on Sunday around 2:00 AM.
11. Instruct the client that they need to leave their system on over night on Saturday nights.
12. Install a firewall and instruct the user on it's use.
13. Run Regclean to clean the registry (**Note:** You may not want to use regclean if this is a fresh install seeing that MS Office will not load properly if regclean is run prior to all of the applications having been installed.) (Regclean is no longer supported by and downloads have been taken off Microsoft's web site.)
14. Connect to the Internet, download and install all Windows Updates.
15. Set "Windows Automatic Updates" to run at your discretion.
16. Download and install **all** Anti-virus and Anti-spyware updates.

17. Run "Disk cleanup"
18. Run "Defrag"
19. Turn "System Restore" back on.
20. Set a "Restore Point"
21. If you have the software (such as Ghost), you could make a bootable "Restore CD" for the client.

Feel comfortable with editing the registry?

More Power: Registry Hacks to Speed Up XP

(System Performance)

Put your Registry-hacking knowledge to good use: hack your way to running Windows XP at top speed.

Creating and marketing tuning and customization utilities for the Windows XP operating system is quickly becoming big business. A Google search will turn up hundreds of sites and programs dedicated to tweaking Windows XP. But no matter what type of interface is developed to make system tweaking easier and safer for the average user, the end result is that the changes are reflected in XP by modifying the Registry. For some people, commercial tweaking utilities might be the method of choice, but with a few precautions and safeguards it's possible to enhance system performance using only those tools supplied with Windows XP.

You can use the Registry Editor to edit the Registry. Make sure you take the precautions outlined in that chapter and back up your Registry, no matter how comfortable you are editing the thing.

No single tweak is going to take an ancient PC and turn it into a gamer's dream machine. It's even unlikely that a number of tweaks will achieve substantial performance gains, but every little bit does help. As long as you keep your expectations realistic, you'll learn something about the Registry and hopefully see a performance increase in the process.

Menu Speed:

When XP first appeared, there was a lot of conversation about the new interface, both good and bad. In spite of the initial complaints, most users stick with the default settings rather than reverting to the Classic interface found in previous Windows versions. But you might want to change the delay you notice when you click the Start menu. I see no reason for there to be any delay when I click the Start menu. Effects are pretty, but I wouldn't click it if I didn't have business inside, so let's get it open and get moving. The default speed can be adjusted with a quick Registry hack.

Go to the Registry key **HKEY_CURRENT_USER\Control Panel\Desktop\MenuShowDelay**. The default value is 400. Set it to 0 to remove the delay completely, but if you do that it will be nearly impossible to move the mouse fast enough not to activate All Programs if you mouse over it en route to your final selection. Pick a number that suits your style, make the change, and then test it until you find a good compromise between speed and usability. (*personal recommendation is 100*)

Place Windows Kernel into RAM:

It's a given that anything that runs in RAM will be faster than an item that has to access the hard drive and virtual memory. Rather than have the kernel that is the foundation of XP using the slower Paging Executive functions, use this hack to create and set the DisablePagingExecutive DWORD to a value of 1.

******Perform this hack ONLY if the system has 256MB or more of installed RAM!******

Edit the Registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\DisablePagingExecutive** to 1 to disable paging and have the kernel run in RAM (set the value to 0 to undo this hack). Exit the Registry and reboot.

Alter Prefetch Parameters:

Prefetching (the reading of system boot files into a cache for faster loading) is a commonly overlooked component that can have a significant impact on system boot time. This tweak allows you to select which components will make use of the prefetch parameters. To see which files are gathered using each setting, clear the prefetch cache located at C:\Windows\Prefetch and then enable one of the settings listed in this hack. Clear the cache and repeat for each setting.

Set the Registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher** to 0 to disable prefetching, 1 to prefetch application launch files, **2 to prefetch boot files** (*personal recommendation*), or 3 to prefetch as many files as possible.

Disable 8.3 Name Creation in NTFS:

Files that use the 8.3 naming convention can degrade NTFS drive performance. Unless you have a good reason for keeping the 8.3 naming convention intact (such as if you're using 16-bit programs), a performance gain can be achieved by disabling it. Set the Registry DWORD key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation** to 1. (*I do not usually change this setting*)

Exit the Registry and reboot.

Summary of "regedit"s:

- 1. HKEY_CURRENT_USER\Control Panel\Desktop\MenuShowDelay - - - set to 100**
- 2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\DisablePagingExecutive - - - set to 1 **only if more than 256MB of RAM****
- 3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher - - - set to 2**