

# Fix Slow PC's Especially Windows XP and Vista

OK so the PC's is running slow.

You are tempted to blame your ISP but in reality it might be a virus, not enough RAM (ie memory), or just too much junk on the system that it's slowed to a crawl.

Windows has a tendency to get clogged up with extraneous services and things running that you just do not need.

If someone has rang you about your slow PC and wants to help you, hang up! Go to point 5 below and run these anti malware programs. Then run your normal antivirus program thoroughly.

Also consider [Microsoft's Safety Scanner](#)

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

Follow the points below if your PC is running slow. It might be infected with something or it might just be clogged with lots of useless stuff and a fragmented disk and/or registry.

## What to Do?

This was written and researched for Vista but equally applies to XP and Windows 7.

Try and clean up your vista setup. See for a good guide <http://www.hl7.com.au/Fix-Optimize-Slow-Windows-Vista.htm> (I would use their AVG reccos. Other options as below)

OK. It's a bit technical! Then follow the points below 1 through to 5:

1. Create a restore point before going further so you can recover and restore to the start point of now. Ok how do I do this. START>CONTROL PANEL>SYSTEM & SECURITY>SYSTEM>SYSTEM PROTECTION>and select your operation system disk and choose SYSTEM RESTORE and give it an appropriate name

2. The following is some good advice on improving Vista. It covers using both the MSCONFIG checking functions, defrags the HDD and does a registry clean

### Vista running incredibly slow (after update)

Click START > RUN > msconfig (comment: look under what starts and in the services TAB and see what sorts of things are starting up. Look for suspicious things) click the "startup" tab uncheck everything except your antivirus (keep a record of what was ticked for future ref: ie screen dump into doc might be good enough) restart your computer.

*OK if you couldn't see the RUN command (right click on the START button and select properties, then Customise Start Menu. About 70% down the list click in the RUN Command box and select OK.*

Right Click "My Computer or Computer" on the desktop, then select your main drive, right click, select properties then tools. Defrag the main drive. Even if it tells you it doesn't need it, defrag it anyways.

Run a Registry cleaner, you can get a good one free from here: <http://www.ccleaner.com/download> clean the junk files and repair the registry. Restart again and give it another whirl.

Note you'll need to go back into MSCONFIG and tick things to auto start them in future

3. You can also go through Control Panel into SYSTEM and then ADVANCED SETTINGS or similar PERFORMANCE> ADVANCE and check Virtual Memory. You might need to increase the Paging file size. Not sure but it should be 2GB if your PC has 2GB RAM. In XP you will manually have to increase it but Vista and Win7 can typically manage it OK.

See <http://www.howtogeek.com/howto/windows-vista/understanding-windows-vista-paging-file-size/>

This tells you some thing about Nortons affecting memory <http://www.computing.net/answers/windows-vista/vista-running-very-slow/6664.html>

4. You can also go through a laborious process of turning off services through Task Manager that are not needed.

[http://news.cnet.com/8301-13880\\_3-9845899-68.html](http://news.cnet.com/8301-13880_3-9845899-68.html)

[http://hubpages.com/hub/How\\_To\\_Turn\\_Off\\_Vistas\\_Useless\\_Junk\\_And\\_Speed\\_Up\\_Your\\_PC](http://hubpages.com/hub/How_To_Turn_Off_Vistas_Useless_Junk_And_Speed_Up_Your_PC)

5. Try out these two free anti malware programs and update them and run a full scan on the C drive. Go and have coffee. Maybe 10 cups or a good book. OK a bottle of wine.

I'd possibly do this step first before anything else.

### **[Super Antispyware 5](#)**

[http://www.filehippo.com/download\\_superantispyware/](http://www.filehippo.com/download_superantispyware/)

SUPERAntiSpyware Professional features advanced Real-Time Protection to ensure protection from installation or re-installation of potential threats as you surf the Internet.

### **[Malware bytes Anti-Malware 1.5](#)**

[http://www.filehippo.com/download\\_malwarebytes\\_anti\\_malware/](http://www.filehippo.com/download_malwarebytes_anti_malware/)

Malwarebytes' Anti-Malware can detect and remove malware that even the most well known anti-virus and anti-malware applications fail to detect. Malwarebytes' Anti-Malware monitors every process and stops malicious processes before they even start.

If you want to try Microsoft Security essential in lieu of Nortons or AVG its free here

[http://www.microsoft.com/security\\_essentials/?mkt=en-us](http://www.microsoft.com/security_essentials/?mkt=en-us)

6. If the issue is your ISP then you'll have to ring them. Maybe others are having problems as well.

For future reference

### **[Simple Guide to Fixing These Issue and Keeping Them Fixed](#)**

1. Adequate memory (XP needs 2GB, Vista can also run on 2GB but more is better, Windows 7 definitely need at least 3GB; 4GB is typical for a 32 bit system. Some with 64 Bit system like 6GB) If you have 1GB it will be very slow. Have run XP, Vista and 7 with 1GB and they will work but are very slow.
2. Regular maintenance, ie backing up critical data, cleaning off things not needed, ensuring updates are installed, including antivirus programs and using them
3. Ensure you have adequate password protection
4. Never give out your details (including credit cards) to strangers
5. Don't allow others to take over your PC or install programs
6. Be careful what site you click on. If you do click on something suspicious then run the anti-malware programs forthwith (and before you log on to your bank)

## Password Security and Password Managers

You should also read and comprehend Password Security and Password Managers below.

# Internet Password Security (including Password Managers)

[Lifehacker](http://lifehacker.com/5530702/best-password-manager-keepass) (<http://lifehacker.com/5530702/best-password-manager-keepass>) rates the best password managers 4th May, 2010. They ran a poll of 5 top contenders and let the users advise through voting. KeePass was voted the best with 33% of the vote. LastPass and 1Password were also rated well, with RoboForm also rated.

[Borntechie](http://www.borntechie.com/entry/10-best-password-manager-utilities-countdown/) (<http://www.borntechie.com/entry/10-best-password-manager-utilities-countdown/>) rates the best 10 best password manager utilities countdown. They rate KeePass as the best

[FilterJoe's](http://www.filterjoe.com/2010/05/14/which-password-manager/) (<http://www.filterjoe.com/2010/05/14/which-password-manager/>) Best Password Manager site and reviews. Also defines what you need in a password manager

[Wikipedia](http://en.wikipedia.org/wiki/Password_manager) ([http://en.wikipedia.org/wiki/Password\\_manager](http://en.wikipedia.org/wiki/Password_manager)) has a small article on password managers

## Free Password Managers Options

[Keepass](http://keepass.info/) (<http://keepass.info/>) Password Safe is a free password manager and worth looking at. It manages the password for the Windows network logon, your e-mail account, your FTP password, online passwords (like website member accounts), etc. KeePass doesn't come with built-in browser integration, but you can invoke a global, auto-login keyboard shortcut (Ctrl+Alt+A by default) when KeePass is running in your system tray. There are two versions of KeePass with 2.1 being the best but does require Microsoft Net Framework >2.0. This is definitely worth considering and as its free maybe should be at the top of our choices. It can be used with Dropbox to provide a nice synchronised solution for multiple machines.

[LastPass](https://lastpass.com/) (<https://lastpass.com/>) is definitely worth considering as its free and supposedly does all that RoboForm does. It works in Firefox, Internet Explorer, Chrome and Safari (Mac) and acts as a password manager for all your web logons. LastPass is gaining recognition as an excellent and secure system. [See Lifehackers Guide to mastering password with LastPass](http://lifehacker.com/5645162/the-intermediate-guide-to-mastering-passwords-with-lastpass?skyline=true&s=i) (<http://lifehacker.com/5645162/the-intermediate-guide-to-mastering-passwords-with-lastpass?skyline=true&s=i>)

You can import from most major password storage vendors (such as RoboForm, 1Password, KeePass, Password Safe, MyPasswordSafe, Skipper, TurboPasswords, Passpack, Firefox and Internet Explorer's built-in password manager) and export too.

Your sensitive data is encrypted using 256bit AES locally before upload so even LastPass cannot get access to it. Please see <https://lastpass.com/technology.php> for more details on our Host Proof Hosting methods that make this safer than you thought possible. Note that encrypted passwords are stored on central servers. Passwords are also encrypted and stored locally on your machine.

How to Update your Insecure Passwords and make them Easy to use. Another [Lifehacker guide](#)

(<http://lifehacker.com/5631203/how-to-update-your-insecure-passwords-and-make-them-easy-to-use>)

## Newsletter Article by Phil (easy logon with password to PC, and RoboForm Password Manager)

As promised at our meeting on 22 January here are a few ideas that will help you avoid internet attacks or loss of identity when using your Windows based PC or laptop whilst connected to the Internet. I hope you find the article which only covers passwords interesting and thought provoking.

There are three main password essentials:

- Have strong passwords for all users of your PC or laptop
- Change these passwords regularly
- Don't use the same password for different sites.

Let's start at the beginning and that is by ensuring that you log in to your computer. Too often, when a user's access is established, no password is entered and the computer is simply allowed to start up without requiring the user to log in. Often this is done to save time but it exposes the Internet connected computer to potentially dangerous hacker activity as a hacker who gains access to your computer does not need to know any password detail before accessing your personal data. This access can involve all your data and the ability to load software onto your PC with a view to trapping keystrokes to access your personal details which can include your banking details, logins and passwords.

You can set up your Windows based computer to automatically start using a predefined user and a predefined password of your choosing each time it is booted. In Windows 7, do the following (if you are using Windows XP or Windows Vista the commands are similar):

Go into Control Panel ->User Accounts and make sure you have allocated a strong password against your User login. Make a note of the User account name and the password. Exit from the Control Panel.

Select 'Run' from the Start Menu after left clicking the 'Start' button.

[If there is no 'Run' option, close down the Start Menu, then right click on the 'Start' button and click on 'Properties'. Then under the 'Start Menu' tab click 'Customise' and then click on 'Run Command'. Exit these menu and go back to the Start Menu and ensure the 'Run' command appears.]

In the dialog box that opens after clicking 'Run' from the Start Menu, enter (without the quote marks) 'control.exe userpasswords2' and hit your 'Enter' key. You should be presented with a 'User Accounts' dialog box. Make sure the 'Users must enter a user name and password to use this computer' checkbox is empty. Click on 'Apply' and a new dialog box opens requiring you to nominate the user and password to be used for automatic log on. Fill in this information and apply the changes.

Your PC or laptop will now automatically log in to the nominated user using the nominated password whenever it is started up. When you change your password you need to repeat these procedure otherwise your PC will continue automatically attempting to log in using the original password.

The strength of your password is important. I can assure you that the use of any word that appears in a dictionary will be cracked by an experienced hacker in a very short time. Click on <https://www.microsoft.com/protect/fraud/passwords/checker.aspx> to get clues on passwords and to check the strength of your chosen password. I guarantee you will be very surprised.

Microsoft recommends that a strong password should appear to be a random row of characters. It should be at least 14 characters long. Where possible it should include a combination of uppercase and lowercase letters, numbers, punctuation, and symbols. It should not be a well-known quote. However, you have to be

able to recall your password and here you need to be a bit more clever. I use the full title of a personal document that I have which includes dates and upper and lower case. You should consider choosing something similar to this but exclude spaces between words and add a few upper case letters and numbers such as might appear in a date.

Ideally you should change your passwords on a regular basis and this means once a month or so, or more often if you suspect your password may have been compromised.

You should have a different password for every Internet site that requires a password for access as you would be crazy to assume that any site will protect your password detail. There are many recorded instances where passwords have been stolen from banks and similar supposedly 'safe' sites. Recently millions of Visa Cards had to be cancelled and re-issues globally due to the theft of personal detail from a US clearing house.

So – always use a different password for every different site you use that requires you to log in and change these regularly particularly where you have bought something on-line and that establishment has details of your credit card or banking details.

Now, how do we keep track of our passwords particularly when we are diligent and regularly change them? Some people open us a Word Document and record these details on their computer. Even if this file is password protected itself, it is not really secure and it is a very 'user-unfriendly' way to record such detail.

Here's a suggestion – use a password control and generation program such as '[RoboForm](#)'.

(<http://www.roboform.com/>) Get the details and try it at no cost.

If you buy this product it will cost you \$US29.95 but it is well worthwhile as you'll appreciate after looking at the video and other information on the above site. I have purchased the product and fully recommend it. It does much more than securely store your varied password detail – it provides a secure repository for unlimited personal information such as tax file numbers, bank account details, magazine subscriptions etc, generates unique strong passwords of any length (eg qX4@HioSmj#r\$j9W81Pr), automatically logs onto your chosen site, and fills out all the detail requested by on-line sites without you having to remember anything other than one master password which is required each session when you use the facility. It remains active for a time you can specify – eg one minute or two hours. It can also work on a USB stick providing identical functionality that can be used on any PC without leaving any traces (extra cost).

I'm sure there are other similar products – I've tried others but none go anywhere near matching the functionality of RoboForm. Sounds like an ad, doesn't it?

If you have any questions on this article, please call Phil

### **End of Phil's Article**

Comments. Excellently conceived article. Most of us probably will struggle with the length of passwords and Phil's idea about the little program are worth considering.

If you let your computer go into sleep mode as is often the case and wise, you will find that the auto log feature won't work and you will be required to enter the PC's password.