



Keep Windows Safe And Up-To-Date

SCUG Windows SIG

April 22, 2010

Keep Windows Safe & Up-To-Date

Windows Update

- Make sure Windows update is set to “Automatic”
- You can set Automatic in Updates from the Windows Control Panel: Windows XP click on the **Performance and Maintenance** category and then on **System**. Select the **Automatic Updates** tab. In Windows Vista click on the **Security** category, next click **Windows Update** and then on **Change Settings**.
- You will get Microsoft Updates on the second Tuesday of each month (also known as 'Patch Tuesday').
- You will have to re-boot your computer for the changes to take effect.

Keep Windows Safe & Up-To-Date

Firewall

- Always run an effective firewall and ensure that it loads automatically at boot time.
- The firewall in Windows XP SP2 and SP3 is more effective than that in SP1, but neither filters outbound traffic (traffic going out from your computer to the Internet).
- In SP2 and SP3 the firewall is ON by default, but in SP1 it is OFF by default.
- In Vista the firewall operates both inbound and outbound, but by default, most outbound filtering in the Windows Vista firewall is turned off .
- A third party firewall is generally considered to be more effective and more configurable and usually works on both inbound and outbound traffic.

Keep Windows Safe & Up-To-Date

Firewall

- Some recommended free firewalls are:
- Comodo
- ZoneAlarm
- Sunbelt Personal Firewall
- There are other firewalls of course: use your personal favourite
- You can check the effectiveness of your firewall at ShieldsUP - your system should be completely 'stealthed'.

Keep Windows Safe & Up-To-Date

Antivirus

- Install antivirus software, keep it updated and always check that it is running when the computer boots up. Schedule a full system scan at least weekly and ensure that the virus definitions are automatically updated. It is recommended that email scanning is enabled in the antivirus software and disabled in your chosen firewall (if the facility to scan email exists there) to avoid possible conflicts. If you need to turn your antivirus off - often advised when installing software - physically disconnect from the Internet first.
- Some recommendations for free antivirus software:
 - * Avira
 - * Avast! 4 Home
 - * AVG Free
- There is other antivirus software of course: use your favourite.

Keep Windows Safe & Up-To-Date

AntiSpyware

- You should always have antispyware software installed on your system and have it scan your system regularly.
- What is Spyware? Spyware is a generic term used for software that behaves in a certain way, such as showing you advertising, collecting your personal information or changing the configuration of your computer, usually without first obtaining your permission to do so.
- Warning: Do not buy or download any antispyware software without first checking the Rogue/Suspect Anti-Spyware Products & Web Sites from Spyware Warrior. At best you get a rogue program that is useless; at worst, they install spyware instead of removing it!
- Here are some good freeware AntiSpyware programs. It is recommended that you have at least two or more installed; they will detect slightly different spyware programs and may miss others.
 - * Microsoft Windows Defender - this provides real time protection against spyware/malware, autoscans and autoupdates.
 - * SpywareBlaster - permanent blocking of over 10,000 known items of spyware, etc. Update manually once a week, but for convenience autoupdate is available for a few dollars.
 - * Spybot Search and Destroy - an on demand scanner with an immunise facility to provide a degree of permanent blocking and works well in conjunction with SpywareBlaster. Update and scan manually once a week.
 - * Ad-Aware - an on demand scanner. Update and scan once a week.
- There are other reputable AntiSpyware programs, so use your favourite.

Keep Windows Safe & Up-To-Date

Internet Explorer

- Windows XP users who have not upgraded to Internet Explorer 7 should do so to take advantage of the enhanced security features - Windows Vista users already have Internet Explorer 7 by default.
- Configure Internet Explorer for maximum security as outlined in this [HelpWithWindows.com Article: How to surf more safely with Internet Explorer 7](#). There is also a version applicable to Internet Explorer 6: [How to surf more safely with Internet Explorer \(Windows XP SP2 version\)](#).
- Set the cookie handling (Tools > Internet Options > Privacy) to Medium High (or High if you prefer).
- Set Internet Explorer to empty the Temporary Internet Files folder when the browser is closed (Tools > Internet Options > Advanced and scroll down to the Security section). For added security place a check mark against Do not save encrypted pages to disk.
- Turn on the popup blocker (Tools > Popup blocker) or use a third party popup stopper - the popup blocker in the Google Toolbar is very effective.
- Turn on the Phishing filter (Internet Explorer 7 only).
- Install IESpyads - a list of restricted sites which help to minimize 'drive by' infections while surfing.
- A further layer of security can be added by installing a custom Hosts file such as the MVPS Hosts File. Alternatively the custom Hosts file in Spybot Search & Destroy may be used.

Keep Windows Safe & Up-To-Date

Firefox

- Set Firefox to automatically download and install updates.
- Update to the newest version when advertised.

Keep Windows Safe & Up-To-Date

Outlook Express/Windows Mail

- Outlook Express For maximum security Outlook Express should be configured so that messages do not automatically open in the Preview pane (View > Layout and uncheck Show Preview Pane). Suspicious emails, particularly those from an unknown source may then be deleted without opening them.
- By default Outlook Express prevents the opening or saving of attachments which could potentially be a virus - in practice this means all attachments - not a very practical solution. The best advice is to enable the opening/saving of attachments (Tools > Options > Security), but to open only those that originate from a known source or are expected. Beware of forwarded emails with attachments.
- More Outlook Express tips in this HelpWithWindows.com TechFile: How to Secure your E-mail against certain viruses

Keep Windows Safe & Up-To-Date

General Security

- The general security of your system may be checked by running the Microsoft Baseline Security Analyser which will highlight any areas in which the system security is compromised and offer solutions to any problems found.
- Remember that the performance of your antivirus and antispyware software will be compromised if the definitions are not kept up to date. Your firewall should also be updated - most have automatic notification of updates.
- It is advisable to keep away from peer to peer (P2P) file sharing sites which are often a source of viruses, etc or at least be aware of the risks involved. Even if you are using a "safe" P2P program, it is only the program that is safe. You will be sharing files from uncertified sources and these are often infected. P2P file sharing is a major conduit used by the 'bad guys' to spread their wares.
- Do not open email attachments from unknown sources.

Keep Windows Safe & Up-To-Date

- **Windows Update**
- **Firewall**
- **Antivirus**
- **AntiSpyware**
- **Internet Explorer**
- **Firefox**
- **Outlook Express/Windows Mail**
- **General Security**

Keep Windows Safe & Up-To-Date

- Questions
- Comments
- Discussion



http://www.helpwithwindows.com/techfiles/Keep_your_Computer_free_from_Viruses_Trojans_Spyware_and_Malware.html