

# XP AntiSpyware 2009 Is a Virus

Tuesday, 28 October 2008

XP AntiSpyware 2009 is an elaborate scam that uses a fake security alert to trick users into clicking it and purchasing protection. XP AntiSpyware 2009 is counterfeit software and it installs spyware onto victim's computers. The infections can be tough to remove manually and there may even be replicators which reproduce them after a reboot.

The most advisable solution is to back up important documents, pictures and music then re-install Windows and all of your applications. If you are unable to do this, here are manual removal instructions which may solve most or all of the problem:

## 1) Kill All Currently Running Instances

- Click ctrl+alt+del on your keyboard. This opens all running processes.
- Click the Processes tab.
- Find AntispywarXP2009.exe and xp\_antispyware.exe and end them both by highlighting each one and clicking the "End Process" button.

## 2) Remove It From Control Panel

- Go to Start --> Control Panel --> Add/Remove Programs and remove XP AntiSpyware 2009.

## 3) Remove Associated Files Manually

- Go to Start --> Search --> All Files or Folders
- Find and delete these files:
- %profile%\application data\secure solutions\AntispywarXP2009\as2008xp.exe
- AntispywarXP2009.exe
- setup\_100527\_3\_.exe
- %profile%\application data\secure solutions\AntispywarXP2009\as2008xp.exe
- setup\_100527\_3\_.exe
- AntispywarXP2009.exe
- ntdll64.dll
- setup.exe
- %desktopdirectory%\AntispywarXP2009.lnk
- %profile%\application data\microsoft\internet explorer\quick launch\AntispywarXP2009.lnk
- %programs%\antispyware 2008\AntispywarXP2009.lnk
- ntdll64.dll
- setup.exe
- antispyware-2009.exe
- \_scui.cpl
- avengn.dll
- %program\_files%\xp\_antispyware\xp\_antispyware.exe
- %programs%\xp\_antispyware\uninstall.lnk
- %programs%\xp\_antispyware\xp\_antispyware.lnk
- %system%\\_scui.cpl
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvcr80.dll
- %program\_files%\xp\_antispyware\pthreadvc2.dll
- %program\_files%\xp\_antispyware\uninstall.exe
- %program\_files%\xp\_antispyware\wscui.cpl
- %program\_files%\xp\_antispyware\xp\_antispyware.cfg
- wini10431.exe
- xp\_antispyware.exe
- %desktopdirectory%\xp\_antispyware.lnk
- %profile%\application data\microsoft\internet explorer\quick launch\xp\_antispyware.lnk
- %program\_files%\xp\_antispyware\avengn.dll
- %program\_files%\xp\_antispyware\comp.dat
- %program\_files%\xp\_antispyware\data\daily.cvd
- install.exe
- %program\_files%\xp\_antispyware\htmlayout.dll
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\microsoft.vc80.crt.manifest
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvc80.dll
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvc80.dll
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvc80.dll
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvc80.dll
- %program\_files%\xp\_antispyware\microsoft.vc80.crt\msvc80.dll

%program\_files%\xp\_antispyware\microsoft.vc80.crt\msvcm80.dll  
%program\_files%\xp\_antispyware\htmlayout.dll  
%program\_files%\xp\_antispyware\avengn.dll  
%program\_files%\xp\_antispyware\pthreadvc2.dll  
%program\_files%\xp\_antispyware\uninstall.exe  
%program\_files%\xp\_antispyware\xp\_antispyware.exe  
wini10431.exe  
install.exe

#### 4) Remove Associated Registry Entries

- Go to Start --> Run... and where it says "Open:" type this: regedit  
- This opens the Windows registry editor. From here you will need to very carefully find and delete some registry entries.  
WARNING: If you do this incorrectly you can cause damage to your system. It is a good idea to back up your registry first. Do this by clicking "My Computer" at the top of the left panel. Then, click File --> Export. Wait for the backup to complete.

- Find and remove these entries:

HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\run ieupdate  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009 lgid  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009 lid  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009 pid  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009\2.1 installtime  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009\2.1 start counter  
HKEY\_CURRENT\_USER\software\secure solutions\AntispywarXP2009\2.1\config

#### 5) Use Anti-Spyware Apps To Remove Leftovers

- Download ComboFix and run it if you feel comfortable using this powerful of an application.  
WARNING: ComboFix can take some time to run. Even if it looks like it is hanging please be patient and do not exit it. You may be prompted to reboot when it is complete. Please do so.  
- Run SpyBot Search & Destroy and Ad-Aware 2008 to find any last remaining remnants.

#### 6) Disable System Restore

- When Windows loads again, go to Start --> Run... and where it says "Open:" type this: services.msc  
- This opens the list of Windows services. Find "System Restore" and right-click it to open a small menu. Then, select "Properties" from the menu.  
- Where it says "Startup type:" use the pulldown menu to select "Disabled".  
- Click the "Stop" button to stop it from running. Stopping and disabling System Restore deletes all previous restore points which may contain the virus. If you roll back to those points, your computer will become infected again.  
- Click the "OK" button.  
- Close the services window.