



bleepingcomputer.com

Home

Forums

Tutorials

Startup List

Spyware Removal

Uninstall List

File Database

Glossary

Resources

Bleeping Computer

Welcome Guide Blogs Chat Help Search RSS

Welcome Guest ([Log In](#) | [Create Account](#))New Member? [Join for free.](#)

Ads by Google

## Spyware Removal Download

Free Spyware Scan. Award-winning Spyware Remover. Download now.

[www.STOPzilla.com](http://www.STOPzilla.com)

### Xp Police Anti Virus?

Don't buy antispysware until you read this  
[spywarefool.blogspot.com](http://spywarefool.blogspot.com)

### Clean Windows XP

Clean out Windows XP in Minutes! 100% Free XP Cleaning  
Download...  
[RegistryCleanerHelp.org](http://RegistryCleanerHelp.org)

### Clean Windows XP Registry

Fix All Windows Errors in 1 Min. Feel The Difference. Free  
Download!  
[quad-cleaner.com](http://quad-cleaner.com)

### Clean Your Windows XP Now

Clean Your Windows XP in 1 Minute. Scan & Repair Your PC  
For Free!  
[Clean-Windows-XP.com](http://Clean-Windows-XP.com)



Ads by Google



Have a problem and would like to ask us for help? To learn how to ask your question [Click Here!](#)



Do you have popups or other malware infecting your computer? If so, [Start Here!](#)



Are you having trouble using this site? Then you should visit the [New User Orientation Center!](#)

► [BleepingComputer.com](#) -> [Malware and Spyware Removal Guides](#)

## How to remove XP Police Antivirus (Removal Guide)

Posted by [Grinler](#) on January 26, 2009 @ 11:01 PM · Views: 12,786



[Add to Favorites!](#)

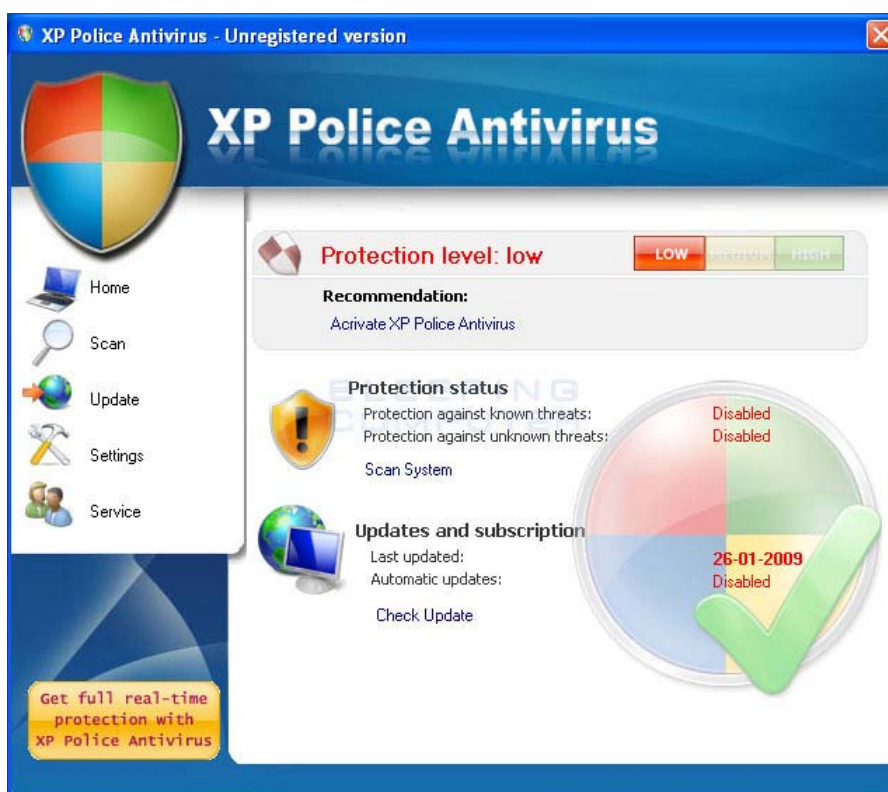


[Print Guide!](#)

### What this programs does:

**XP Police Antivirus** is a new program that attempts to deliberately trick you into thinking you are infected. It does this by displaying [security](#) warnings from your Windows taskbar, by displaying a fake Windows Security Center window, and by showing fake infections after scanning your [computer](#). It is for these reasons that we categorize this program as a rogue [anti-spyware](#) program.

When XP Police [Antivirus](#) is installed on to your computer it will add an entry to your Windows registry so that the program starts automatically when you boot the computer. Once the program is loaded it will automatically scan your computer and list a large amount of infections. These infections, though, cannot be removed unless you first purchase XP Antivirus Police. This is a scam as the infections that are found do not actually exist on your computer. They are only being shown in order to scare you into thinking you are infected and hoping that you will purchase their [software](#).



XP Police Antivirus screen shot  
For more screen shots of this infection click on the image above.  
There are a total of 9 images you can view.

Threat Descriptions

Rogue Programs

Trojan Horses

Worms

Search Guides

Google™ Custom Se

Search

Subscribe

RSS

MY YAHOO!

Google

Windows Live

Technorati

NEWSBURST

BlogRoll

MalwareBytes Blog

While the program is running you may also encounter other undesirable behavior such as:

- When browsing the web in [Internet](#) Explorer you will randomly be shown a page stating that there was "*Insecure Internet activity. Threat of virus attack*". It will then prompt you to either purchase XP Police Antivirus or continue to the page you were requesting. Regardless of the answer you select, it will still open the purchase page for the rogue.
- Alerts pretending to be [firewall](#) alerts stating that your computer is sending hidden data to a remote computer.
- A fake Windows Security Center that states that "*Windows Security center reports that 'XP Police Antivirus' is unable to protect your system*" and that you should purchase the software. This Window is just a fake and is not the actual Windows Security Center and should be ignored.
- A fake alert in the form of a small box appearing above your Windows taskbar stating that your computer is sending unauthorized information to random IP addresses.
- A small balloon alert stating that a Trojan was detected and that you should purchase XP Police Antivirus to protect yourself. The text of this alert is:

**Trojan Detected!**

A piece of malicious code was found in your system which can replicate itself if no action is taken. Click here to have your system cleaned by XP Police Antivirus.

- Your computer beginning to act slower due to XP Police using up your computer's resources while performing the above actions.

If you encounter any of the above alerts, they should all be ignored as they are displaying false information. Instead please use the guide below to remove XP Police Antivirus program and any associated malware for free.

#### Threat Classification:

- [Information on Rogue Programs](#)

**Advanced information:**

[View XP Police Antivirus files.](#)

[View XP Police Antivirus Registry Information.](#)

**Tools Needed for this fix:**

- [Malwarebytes' Anti-Malware](#)

**Symptoms that may be in a HijackThis Log:**

O2 - BHO: WinSafe Class - {b6b571fb-b71d-449c-ad70-82e966328795} - C:\WINDOWS\iehost.dll  
O4 - HKCU\...\Run: [PoliceAV] C:\Program Files\XPPoliceAntivirus\xppolice.exe

**Guide Updates:**

01/26/09 - Initial guide creation.

02/04/09 - Updated guide to include new fake alert and Internet Explorer Hijack.

---

**Automated Removal Instructions for XP Police Antivirus using Malwarebytes' Anti-Malware:**

1. [Print](#) out these instructions as we will need to close every window that is open later in the fix.
2. Download Malwarebytes' Anti-Malware, or MBAM, from the following location and save it to your [desktop](#):  
  
[Malwarebytes' Anti-Malware Download Link](#)
3. Once downloaded, close all programs and Windows on your computer, including this one.
4. Double-click on the icon on your desktop named **Download\_mbam-setup.exe**. This will start the installation of MBAM onto your computer.
5. When the installation begins, keep following the prompts in order to continue with the installation process. Do not make any changes to default settings and when the program has finished installing, make sure you leave both the **Update Malwarebytes' Anti-Malware** and **Launch Malwarebytes' Anti-Malware** checked. Then click on the **Finish** button.
6. MBAM will now automatically start and you will see a message stating that you should update the program before performing a scan. As MBAM will automatically update itself after the install, you can press the **OK** button to close that box and you will now be at the main program as shown below.



7. On the **Scanner** tab, make sure the **Perform quick scan** option is selected and then click on the **Scan** button to start scanning your computer for **XP Police Antivirus** related files.
8. MBAM will now start scanning your computer for malware. This process can take quite a while, so we suggest you go and do something else and periodically check on the status of the scan. When MBAM is scanning it will look like the image below.



9. When the scan is finished a message box will appear as shown in the image below.



You should click on the OK button to close the message box and continue with the **XP Police Antivirus** removal process.

10. You will now be back at the main [Scanner](#) screen. At this point you should click on the **Show Results** button.
11. A screen displaying all the malware that the program found will be shown as seen in the image below. Please note that the infections found may be different than what is shown in the image.



You should now click on the **Remove Selected** button to remove all the listed malware. MBAM will now delete all of the files and registry keys and add them to the programs quarantine. When removing the files, MBAM may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot, please allow it to do so. Once your computer has rebooted, and you are logged in, please continue with the rest of the steps.

12. When MBAM has finished removing the malware, it will open the scan log and display it in Notepad. Review the log as desired, and then close the Notepad window.
13. You can now exit the MBAM program.

Your computer should now be free of the **XP Police Antivirus** program. If your current [anti-virus](#) solution let this infection through, you may want to consider [purchasing the PRO version of Malwarebytes' Anti-Malware](#) to protect against these types of threats in the future.

If you are still having problems with your computer after completing these instructions, then please follow the steps outlined in the topic linked below:

[Preparation Guide For Use Before Posting A Hijackthis Log](#)

#### Associated XP Police Antivirus Files:

```
c:\Program Files\XPPoliceAntivirus
c:\Program Files\XPPoliceAntivirus\AVCoreFn.dll
c:\Program Files\XPPoliceAntivirus\bdconf.cfg
c:\Program Files\XPPoliceAntivirus\Core.dll
c:\Program Files\XPPoliceAntivirus\setup.dat
c:\Program Files\XPPoliceAntivirus\ppolice.exe
c:\Program Files\XPPoliceAntivirus\Plugins
c:\Program Files\XPPoliceAntivirus\Plugins\ceva_dll.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\ceva_emu.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\ceva_vfs.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\ceva_vfs.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\cevakrnl.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\cevakrnl.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\cevakrnl.rvd
c:\Program Files\XPPoliceAntivirus\Plugins\cookie.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\cran.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\cran.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\le_spyw.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\le_spyw.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\lemalware.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\gvmscripts.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\hpe.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\java.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\mdx_97.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\mdx_97.ivd
```

```

c:\Program Files\XPPoliceAntivirus\Plugins\mdx_w95.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\mdx_x95.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\mdx_xf.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\mobmalware.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\na.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\nelf.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\regarch.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\regscan.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\rup.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\sdx.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\sdx.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\unpack.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\unpack.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\vb0.dat
c:\Program Files\XPPoliceAntivirus\Plugins\vb1.dat
c:\Program Files\XPPoliceAntivirus\Plugins\vb2.dat
c:\Program Files\XPPoliceAntivirus\Plugins\ve.cvd
c:\Program Files\XPPoliceAntivirus\Plugins\ve.ivd
c:\Program Files\XPPoliceAntivirus\Plugins\vedata.cvd
c:\Program Files\XPPoliceAntivirus\sounds
c:\Program Files\XPPoliceAntivirus\sounds\alert.wav
c:\Program Files\XPPoliceAntivirus\sounds\click.wav
c:\Program Files\XPPoliceAntivirus\sounds\fire.wav
%UserProfile%\Desktop\XP Police Antivirus.LNK
%UserProfile%\Start Menu\XP Police Antivirus.LNK

```

### Associated XP Police Antivirus Windows Registry Information:

```

HKEY_CURRENT_USER\Software\XP Police Antivirus
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{b6b571fb-b71d-449c-ad70-82e966328795}

```

[Ads by Google](#)

## Spyware Removal Download

Free Spyware Scan. Award-winning Spyware  
Remover. Download now.

[www.STOPzilla.com](http://www.STOPzilla.com)

---

**This is a self-help guide. Use at your own risk.**

BleepingComputer.com can not be held responsible for problems that may occur by using this information. If you would like help with any of these fixes, you can post a HijackThis log in our [HijackThis Logs and Analysis forum](#).

If you have any questions about this self-help guide then please post those questions in our [AntiVirus, Firewall and Privacy Products and Protection Methods forum](#) and someone will help you.

[Advertise](#) | [About Us](#) | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | [Site Map](#) | [Chat](#) | [Tutorials](#)  
[Discussion Forums](#) | [The Computer Glossary](#) | [Resources](#) | [RSS Feeds](#) | [Startups](#) | [The File Database](#) | [Malware Removal Guides](#)

© 2003-2009 All Rights Reserved [Bleeping Computer LLC](#).  
PGT: 0.07666 Queries: 12