

Re: How do I get rid of an aggressive/relentless pop-up?

## Re: How do I get rid of an aggressive/relentless pop-up?

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-12/msg00298.html>

---

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
  - *Date:* Fri, 29 Dec 2006 19:34:00 -0500
- 

From: "alister28" <alister28@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| Thanks for replying. No, it doesn't have "Messenger Service" in the top  
| border. It has the Internet Explorer icon followed by "Your MBS Bill –  
| Windows Internet Explorer". Then below in the information bar it has the  
| address "<https://secure.microbillsys.com/EN/bill.php>. (And yet, when I view  
| my Internet history it is listed there as "<http://auth.microbillsys.com>.  
| Another thing is that it writes an icon onto my desktop with the name "MBS  
| Account Manager". This is what I mean by aggressive and relentless.) In the  
| pop-up window with the address "<https://secure.microbillsys.com/EN/bill.php>,  
| the window has conveniently disabled the "Menu Bar" which makes me completely  
| suspicious. Because the Menu Bar would allow me to investigate the source of  
| the window to determine whether it is malicious or not, but that function has  
| been somehow rendered inoperative/inaccessible. A genuine pop-up window from  
| a legit source – e.g. Sky Television – would normally allow itself to be  
| scrutinised. The only other details I can give you are that the window will  
| not let itself be put into the background, and stands out in front of  
| everything else. It says things like "Secure Internet Billing Solutions", and  
| presents me with various options to pay my bogus bill for a bogus package  
| "Sexxxpassport Subscription for period 27th Dec 2006 – 26th Jan 2007". The  
| company is Micro Bill Systems Ltd. That's all I can see for now. Hope this  
| helps.

|--

| Remember, no matter where you go, there you are.

If you are using any version of Sun Java that is prior to JRE Version 6.0,  
then you are strongly urged to remove any/all versions.  
There are vulnerabilities in them and they are actively being exploited.

It is highly suggested that you update to the latest version which is Sun Java JRE/JSE  
Version 6.0

Simple check, look under...  
C:\Program Files\Java

Re: How do I get rid of an aggressive/relentless pop-up?

Re: How do I get rid of an aggressive/relentless pop-up?

The only folder under that folder should be the latest version.

Such as...

C:\Program Files\Java\jre1.6.0

<http://java.sun.com/javase/downloads/index.jsp>

<http://www.java.com/en/download/manual.jsp>

FYI:

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102557-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102622-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102648-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102729-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102732-1>

For non-viral malware...

Please download, install and update the following software...

\* Ad-aware SE v1.06

<http://www.lavasoft.de/>

<http://www.lavasoftusa.com/>

<http://www.lavasoft.de/ms/index.htm>

\* SpyBot Search and Destroy v1.4

<http://security.kolla.de/>

<http://www.safer-networking.org/microsoft.en.html>

\* SuperAntiSpyware

<http://www.superantispyware.com/superantispywarefreevspro.html>

After the software is updated, I suggest scanning the system in Safe Mode.

I also suggest downloading, installing and updating BHODemon for any Browser Helper Objects that may be on the PC.

\* BHODemon

<http://www.majorgeeks.com/downloadget.php?id=3550&file=11&evp=245a87539eea8ed6904332b4b8b8442d>

For viral malware...

\* Download MULTI\_AV.EXE from the URL ---

[http://www.ik-cs.com/programs/virttools/Multi\\_AV.exe](http://www.ik-cs.com/programs/virttools/Multi_AV.exe)

To use this utility, perform the following...

Execute: Multi\_AV.exe { Note: You must use the default folder C:\AV-CLS }

Choose: Unzip

Choose: Close

Re: How do I get rid of an aggressive/relentless pop-up?

Re: How do I get rid of an aggressive/relentless pop-up?

Execute: C:\AV-CLS\StartMenu.BAT  
{ or Double-click on 'Start Menu' in C:\AV-CLS }

NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your FireWall to allow it to download the needed AV vendor related files.

C:\AV-CLS\StartMenu.BAT -- { or Double-click on 'Start Menu' in C:\AV-CLS }  
This will bring up the initial menu of choices and should be executed in Normal Mode.  
This way all the components can be downloaded from each AV vendor's web site.  
The choices are: Sophos, Trend, McAfee, Kaspersky, Exit this menu and Reboot the PC.

You can choose to go to each menu item and just download the needed files or you can download the files and perform a scan in Normal Mode. Once you have downloaded the files needed for each scanner you want to use, you should reboot the PC into Safe Mode [F8 key during boot] and re-run the menu again and choose which scanner you want to run in Safe Mode. It is suggested to run the scanners in both Safe Mode and Normal Mode.

When the menu is displayed hitting 'H' or 'h' will bring up a more comprehensive PDF help file. <http://www.ik-cs.com/multi-av.htm>

Additional Instructions:  
[http://pcdid.com/Multi\\_AV.htm](http://pcdid.com/Multi_AV.htm)

\* \* \* Please report back your results \* \* \*

==

Dave  
<http://www.claymania.com/removal-trojan-adware.html>  
<http://www.ik-cs.com/got-a-virus.htm>

.

Re: How do I get rid of an aggressive/relentless pop-up?