


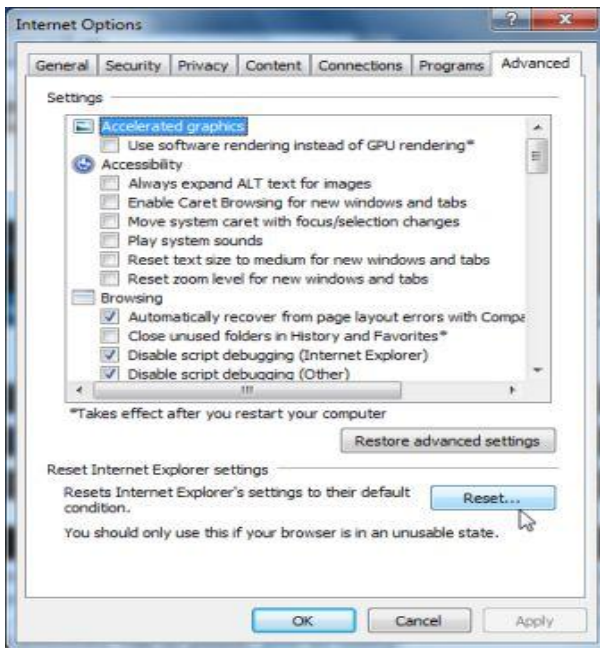
Please note: Applying these steps will delete any private settings / temporary files. Like home page reset, temporary internet files, history etc. Because Malware could be attacking from any of this place.

Remove Pop-up Ads from Internet Explorer

1. Open Internet Explorer, click on the **gear icon**  (*Tools* for Windows XP users) at the top (far right), then click again on **Internet Options**.



2. In the *Internet Options* dialog box, click on the **Advanced** tab, then click on the **Reset** button.



3. In the *Reset Internet Explorer settings* section, check the **Delete personal settings** box, then click on **Reset**.

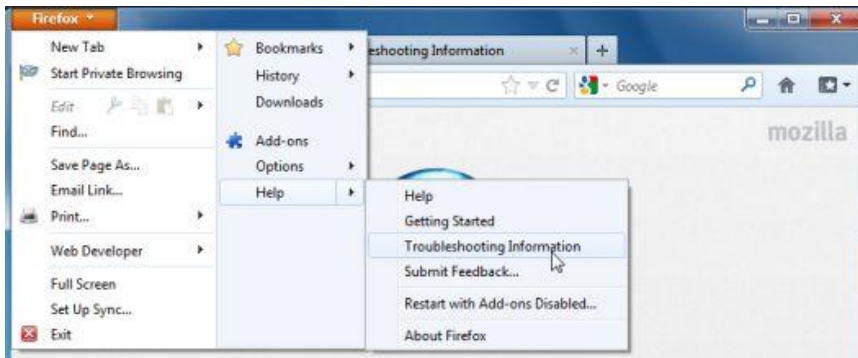


4. When Internet Explorer finishes resetting, click **Close** in the confirmation dialogue box and then click **OK**.

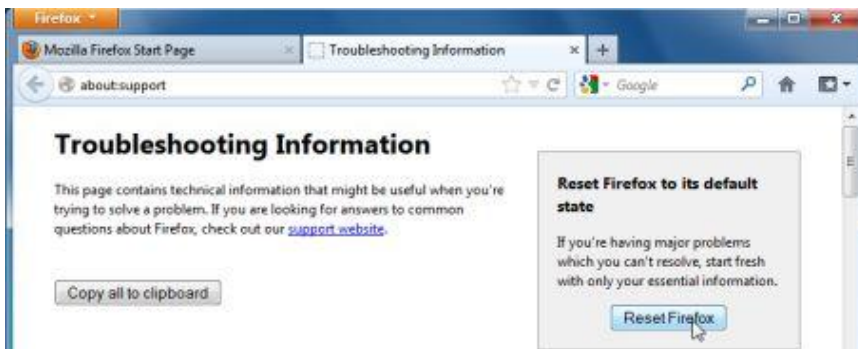
5. **Close and Restart Internet Explorer.**

Remove Pop-up Ads from Mozilla Firefox

1. At the top of the Firefox window, click the **Firefox button**, go over to the **Help** sub-menu (on *Windows XP*, click the Help menu at the top of the Firefox window), and select **Troubleshooting Information**.



2. Click the **Reset Firefox** button in the upper-right corner of the *Troubleshooting Information* page.

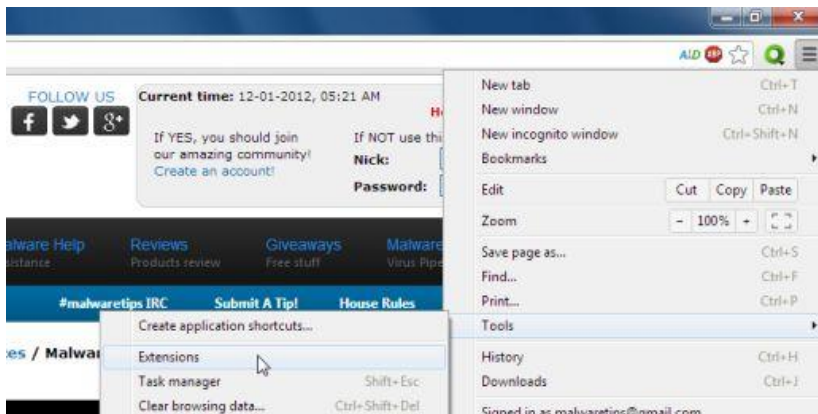


3. To continue, click **Reset Firefox** in the confirmation window that opens.
4. Firefox will close and be reset. When it's done, a window will list the information that was imported. Click **Finish**.

Remove Pop-up Ads from Google Chrome

1. Remove the malicious extensions from Google Chrome.

Click the Chrome menu  button on the browser toolbar, select **Tools** and then click on **Extensions**.



2. In the **Extensions** tab, remove (by clicking on the Recycle Bin) the **LyricsSay-1, LyricXeecker, HD-Plus, GetLyrics, DownloadTerms 1.0, Browse2Save, TidyNetwork.com, WebCake** and any other unknown extensions from Google Chrome. Basically, if you have not installed an extension, you should remove it from your web browser.

Chrome

- History
- Extensions**
- Settings
- Help

Extensions Developer mode

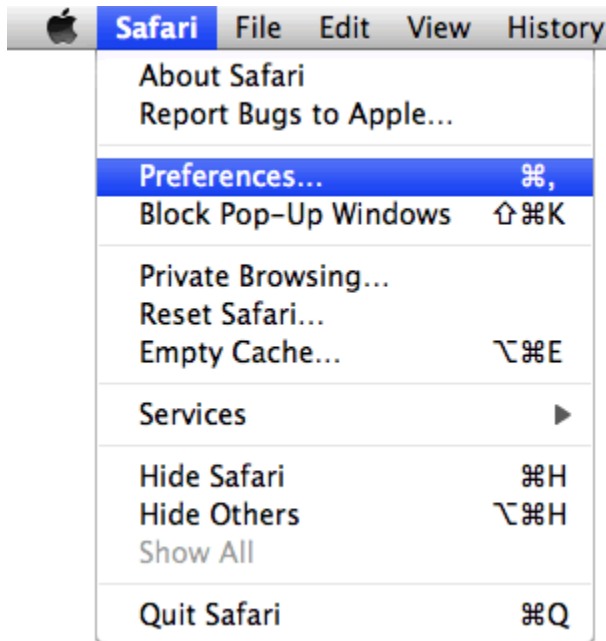
	DefaultTab 1.1.1.19 In order to remove Default Tab installation go to control panel -> Add/Remove Programs (xp) or Programs and Features (vista and above) -> Default Tab Permissions <input type="checkbox"/> Allow in incognito <input type="checkbox"/> Allow access to file URLs	<input checked="" type="checkbox"/> Enabled  Installed by a third party.
	DownloadTerms 1 Find word meanings passively Permissions <input type="checkbox"/> Allow in incognito <input type="checkbox"/> Allow access to file URLs	<input checked="" type="checkbox"/> Enabled  Not from Chrome Web Store.
	LessTabs 1.7.1.0 LessTabs = Mo Time! Permissions Visit website <input type="checkbox"/> Allow in incognito Options	<input checked="" type="checkbox"/> Enabled  Not from Chrome Web Store.
	TidyNetwork.com 4.0.0.0 No description Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled  Not from Chrome Web Store.
	WebCake 1.0.3 Add WebCake to your web experience. Permissions <input type="checkbox"/> Allow in incognito <input type="checkbox"/> Allow access to file URLs	<input checked="" type="checkbox"/> Enabled  Installed by a third party.

3. Close and Restart your browser.

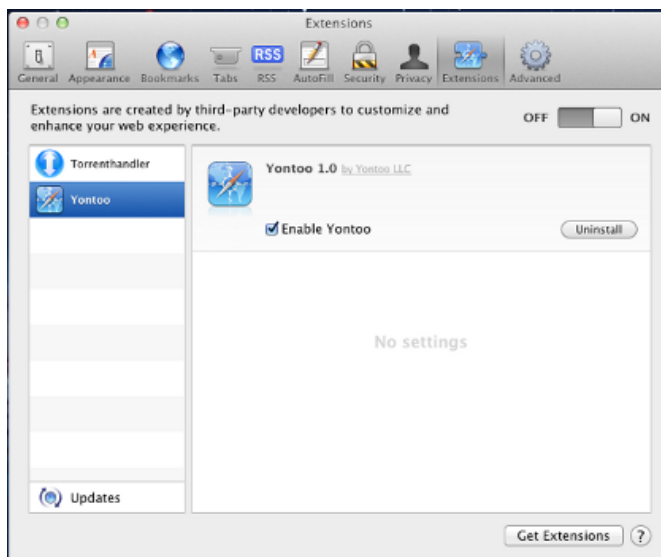
Remove Pop-up Ads from MAC

Remove malicious extension from Safari

1. From the Safari menu, select “Preferences”.



2. In the Safari Preferences window, click the “Extensions” tab. Find any malicious plugin, then click on the “Uninstall” button.



In case, problem won't get resolved with above steps; please follow below instructions.

Reset Safari to prevent other users of your computer from seeing information about how you used Safari. You can also reset to try to solve problems with opening webpages.

Warning: When you reset Safari, it deletes the browsing history it stored for you, but doesn't delete the browsing history stored by some plug-ins you may have installed.

1. Choose Safari > Reset Safari.
2. Deselect items you don't want to reset:

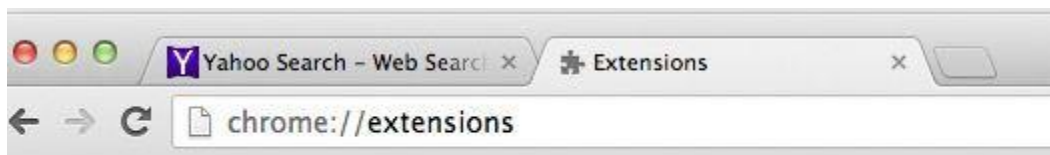
Option	Description
Clear history:	Clears the list of webpages you viewed, empties caches, removes website icons, and clears the list of recent searches. Also clears managed website settings for all plug-ins with websites set to Block Always. Website icons, also called favicons, appear in the search and address field and other places. You see your recent searches by clicking the magnifying glass at the left end of the search and address field when it's empty.
Reset Top Sites:	Clears changes you made to Top Sites, such as adding or pinning sites. If you also clear your history, your Top Sites page reverts to the webpage previews displayed when you first installed Safari.
Reset all location warnings:	Removes information that websites saved about your location.
Reset all website notification warnings:	Removes the record of websites that you allowed or denied permission to post Notification Center alerts. This option is shown in OS X v10.8 or later.
Remove all website data:	Removes cookies, tracking information, and other data that websites stored on your computer. Also clears all managed website settings for plug-ins.
Clear the Downloads window:	Clears the list of files you downloaded in Safari. The files remain on your computer until you delete them.


Option	Description
Close all Safari windows:	Closes all windows thereby preventing another user from viewing webpages you visited.

3. Click Reset.

Remove malicious extensions from Google Chrome

1. In Chrome address bar, type *chrome://extensions*
















2. On the *Extensions* window, remove the **MacVX**, **Amazon Shopping Assistant**, **Domain Error Assistant**, **Ebay Shopping Assistant**, **Searchme**, and **Slick Savings** and any other unknown extensions by clicking the trash can  icon.

Chrome
History
Extensions
Settings
Help

chrome://extensions

Extensions Developer mode

	Amazon Shopping Assistant by Spigot 1.0 Get the best deals on Amazon.com Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 
	Domain Error Assistant 1.1 Domain Error Assistant Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 
	Ebay Shopping Assistant by Spigot 1.0 Get the best deals on Ebay.com Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 
	[Redacted] <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 
	Searchme 1.1 Search the web with Searchme Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 
	Slick Savings 2.4 Slick Savings will help you save money when shopping online. When alerted that there are coupons available, simply click on "View All Available Coupons" for all the deals on the site you're browsing. Click the coupon to apply automatically! Coupons are provided by Savings-Slider. Savings-Slider is ad-supported software that is provided at no cost and may display advertisements in websites as you view them. Permissions <input type="checkbox"/> Allow in incognito	<input checked="" type="checkbox"/> Enabled 

 [Get more extensions](#) [Keyboard shortcuts](#)

Remove malicious extensions from Firefox

1. In Firefox, click the “**Tools**” menu, then click “**Add-ons**”.
2. Select the **Extensions** tab, then remove **MacVX**, **Amazon Shopping Assistant**, **Domain Error Assistant**, **Ebay Shopping Assistant**, **Searchme**, and **Slick Savings** and any other unknown extensions from Mozilla Firefox.

