Malwarebytes

Why did we send you here?

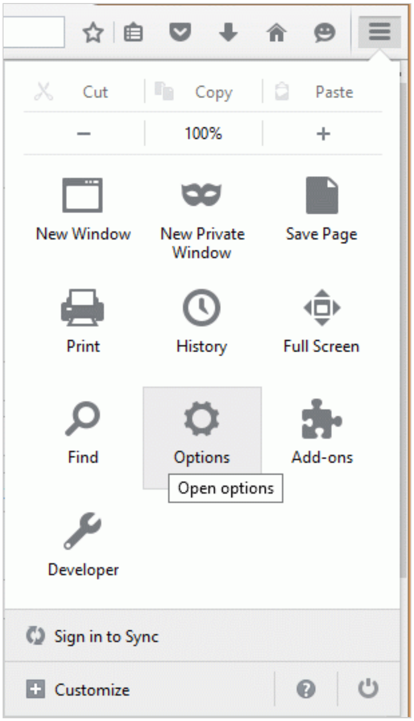
During your last scan, we found some infections that have caused changes on your system, which may need to be manually altered. We'll show you how to do that on this page.

Our instructions are divided into three chapters:

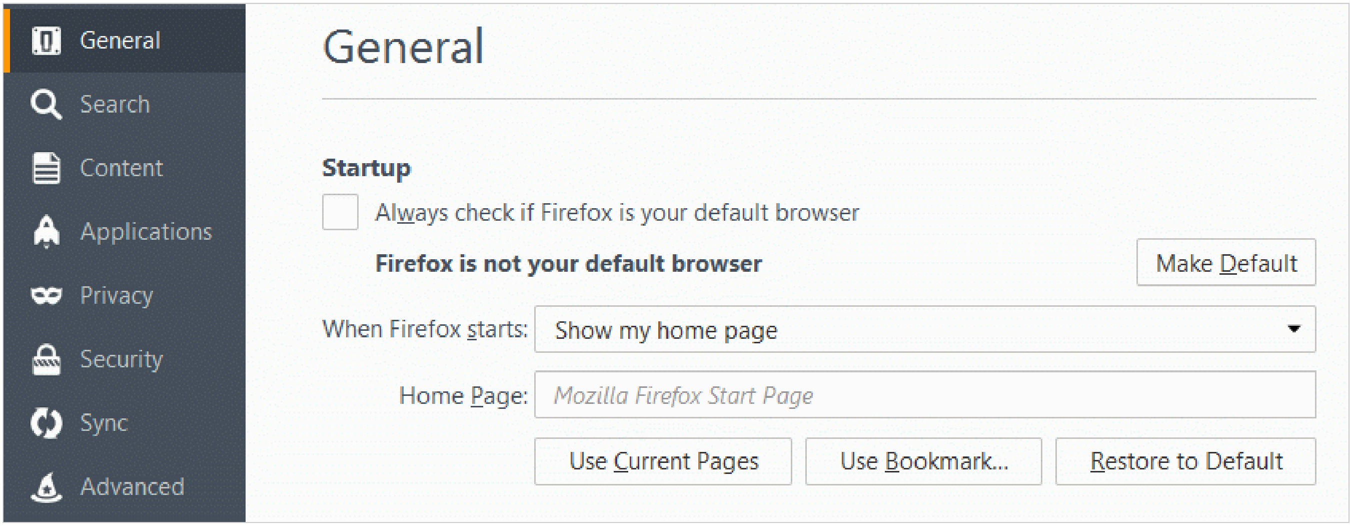
- How to restore start pages, search engines, and other settings in Firefox
- How to restore start pages, search engines, and other settings in Google Chrome
- How to fix browser shortcuts for Firefox, Chrome, and Internet Explorer

How to restore start pages, search engines, and other settings in Firefox

Click the "Open menu" button and choose "Options."



On the "General" tab under "Startup," use one of the buttons or manually change the URL in the "Home Page" field.



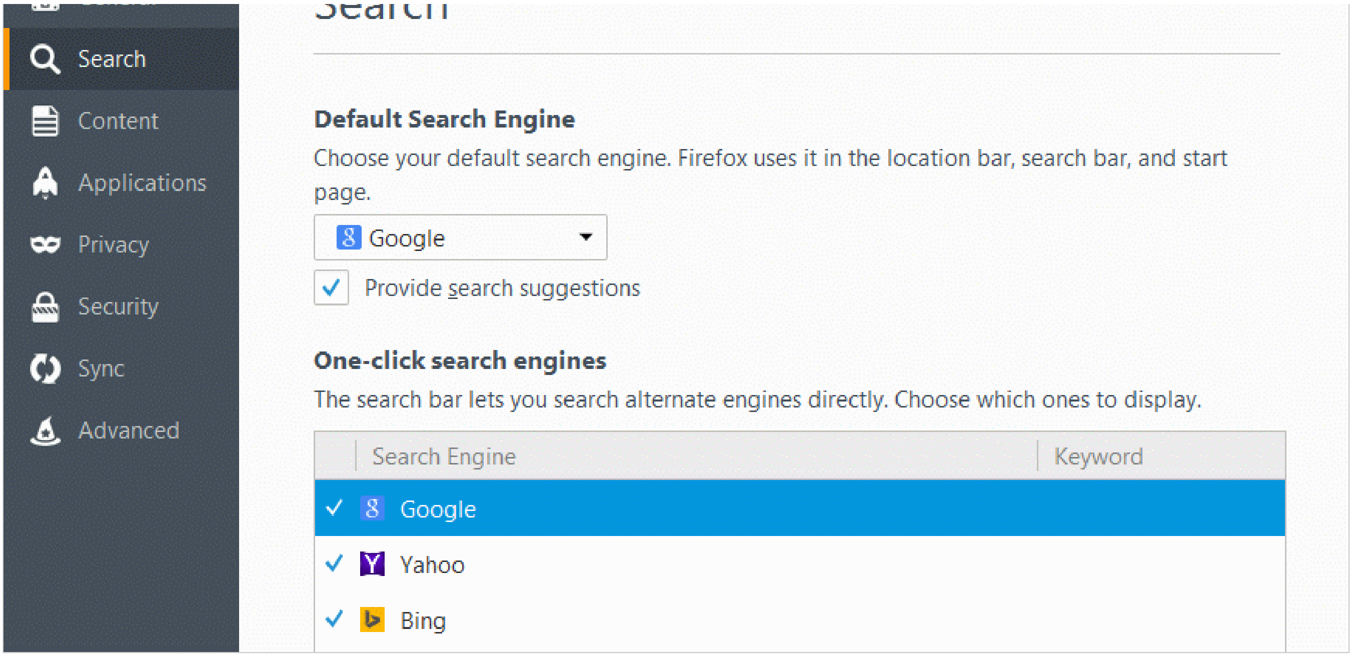
□ Always check if Firefox is your default browser

Firefox is not your default browser Make Default

When Firefox starts: Show my home page

Home Page: *Mozilla Firefox Start Page*

On the "Search" tab, you can choose your default search engine and which search providers should be displayed as alternate engines.



Search

Default Search Engine

Choose your default search engine. Firefox uses it in the location bar, search bar, and start page.

Google

☑ Provide search suggestions

One-click search engines

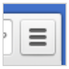
The search bar lets you search alternate engines directly. Choose which ones to display.

	Search Engine	Keyword
✓	Google	
✓	Yahoo	
✓	Bing	

On the “Sync” tab, you can click on “Unlink this device” if you don’t want other devices to inherit the changes from the one you are working on (and vice versa).

In extreme cases, it might be necessary to uninstall Firefox and make a fresh start. If you do that because of the effects of an infection, we advise you to follow the “Remove user data and settings” instructions. If you want to transfer your bookmarks to the new setup, you can follow these directions.

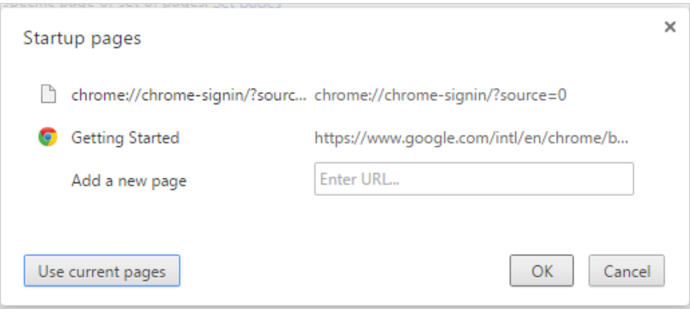
How to restore start pages, search engines, and other settings in Google Chrome



Click the button that opens the “customize and control” menu in Chrome.

Then click “Settings.” Scroll down in the Settings menu to “On startup.”

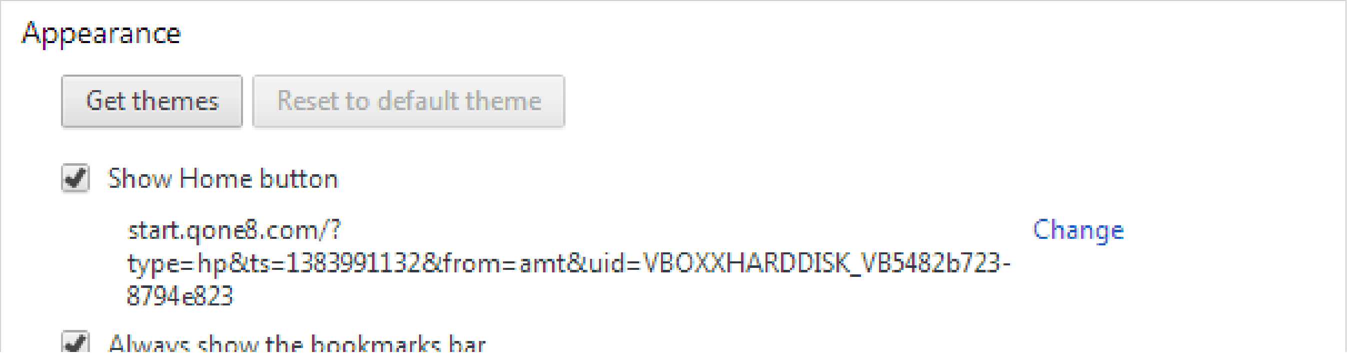
Under “On startup,” you can change the pages that Chrome opens with by clicking the “Set pages” link next to the “Open a specific page or set of pages” option.



Startup pages

chrome://chrome-signin/?sourc...	chrome://chrome-signin/?source=0
Getting Started	https://www.google.com/intl/en/chrome/b...
Add a new page	Enter URL...

Under “Appearance,” click the “Change” link beside the “Show Home button” option to alter the URL that will open when that button is used.

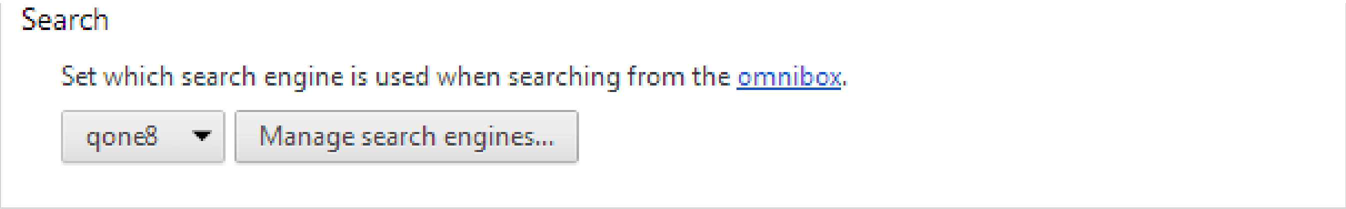


Appearance

☑ Show Home button

start.qone8.com/?type=hp&ts=1383991132&from=amt&uid=VBOXXHARDDISK_VB5482b723-8794e823 Change

☑ Always show the bookmarks bar

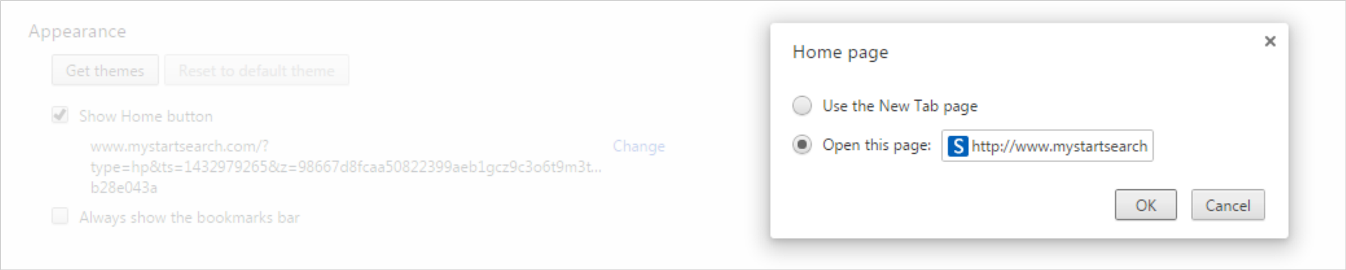


Search

Set which search engine is used when searching from the omnibox.

qone8 ▼ | Manage search engines...

You can edit the URL in the resulting pop-up screen.



Appearance

Get themes | Reset to default theme

☑ Show Home button

www.mystartsearch.com/?type=hp&ts=1432979265&z=98667d8fcaa50822399aeb1gcz9c3o6t9m3t... b28e043a Change

□ Always show the bookmarks bar

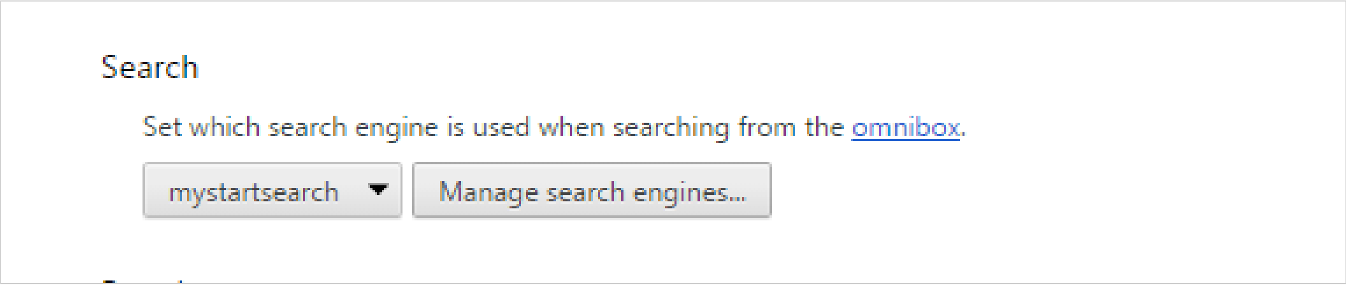
Home page ×

○ Use the New Tab page

● Open this page: http://www.mystartsearch

OK | Cancel

Under "Search," you can decide which search engine to use when you search from the omnibox.

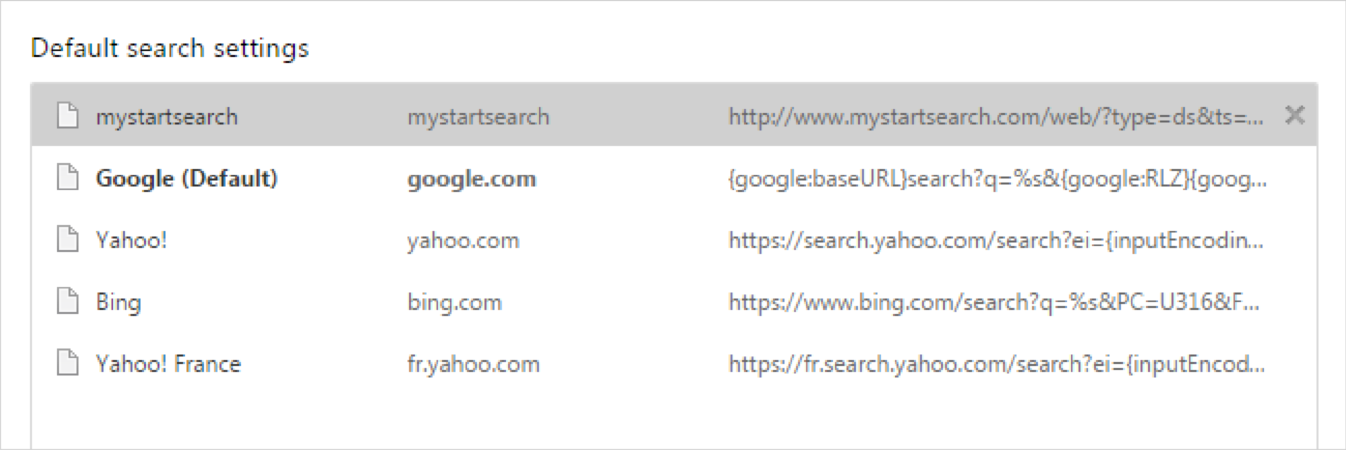


Search

Set which search engine is used when searching from the omnibox.

mystartsearch ▼ | Manage search engines...

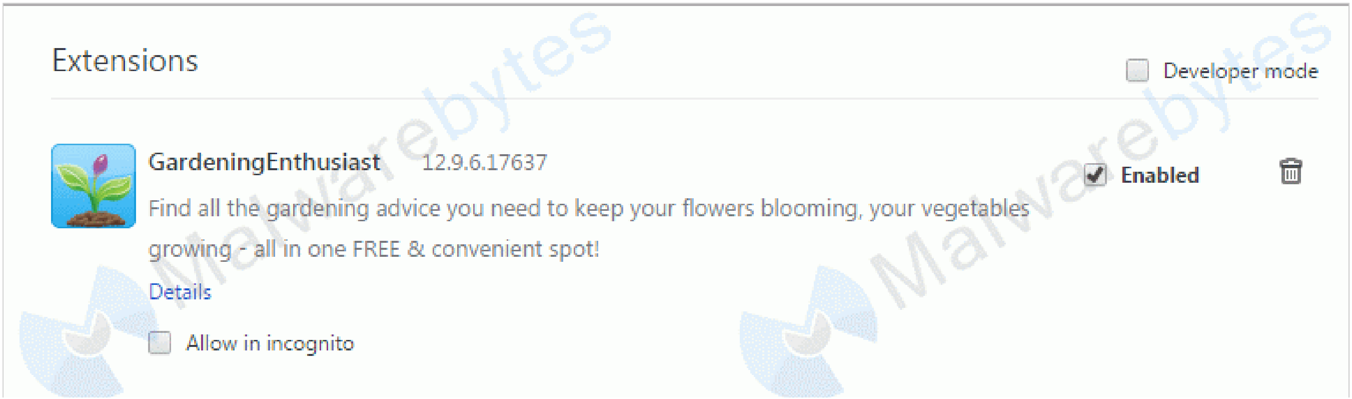
Click the "Manage search engines..." button to select the default search engine. Remove unwanted entries by clicking on the (**X**) next to an entry.



Default search settings

mystartsearch	mystartsearch	http://www.mystartsearch.com/web/?type=ds&ts=... ✕
Google (Default)	**google.com**	{google:baseURL}search?q=%s&{google:RLZ}{goog...
Yahoo!	yahoo.com	https://search.yahoo.com/search?ei={inputEncodin...
Bing	bing.com	https://www.bing.com/search?q=%s&PC=U316&F...
Yahoo! France	fr.yahoo.com	https://fr.search.yahoo.com/search?ei={inputEncod...

If an (orphaned) extension is left behind, you can remove it manually under "Tools" / "Settings" / "Extensions."



Extensions □ Developer mode

GardeningEnthusiast 12.9.6.17637 ☑ Enabled

Find all the gardening advice you need to keep your flowers blooming, your vegetables growing - all in one FREE & convenient spot!

Details

□ Allow in incognito

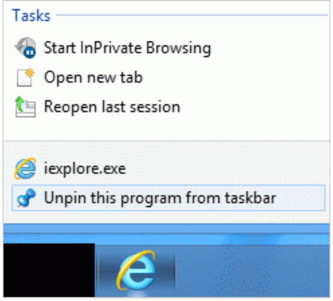
In extreme cases, it might be necessary to do a fresh install. Once you decide it is better to uninstall Chrome, you may want to back up your bookmarks first. To avoid the effects of an infection from carrying over to the new install, you should use the "Also delete your browsing data" checkbox.

Read the instructions for synced data to avoid the spreading the infection to other devices or receiving additional infections from other devices.

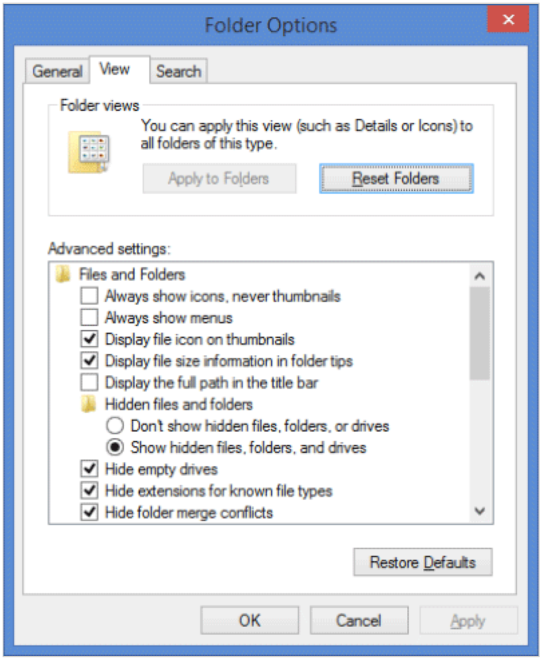
How to fix browser shortcuts for Firefox, Chrome, and Internet Explorer

Sometimes browser hijackers alter the shortcuts on your desktop, taskbar, and start menu in order to make sure you visit their sites or view their advertisements. They do this by adding extra information to the existing shortcuts. Unfortunately, we can't remove the extra information for you, so we'll show you how to create new, clean shortcuts.

If the infected shortcuts are pinned at the taskbar, right-click the icon and choose "Unpin this program from taskbar."



If the "Unpin" method does not work, you can remove the shortcuts from your taskbar in the hidden folder. First, you need to show your hidden files. Go to "Control Panel" / "Folder Options" / "View," and then select "Show hidden files, folders, and drives."



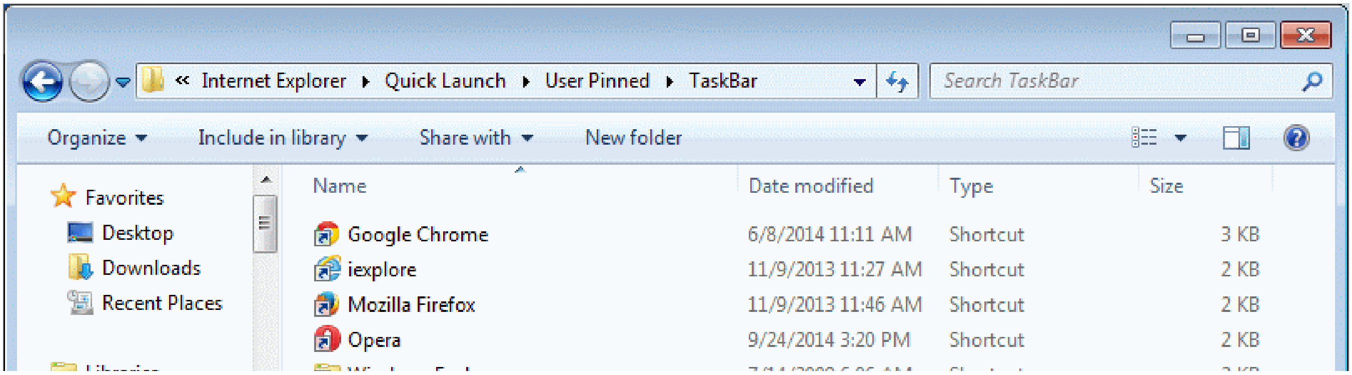
You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

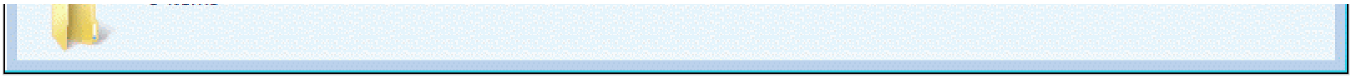
Files and Folders
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar

Hidden files and folders
- ○ Don't show hidden files, folders, or drives
- ● Show hidden files, folders, and drives
- ☑ Hide empty drives
- ☑ Hide extensions for known file types
- ☑ Hide folder merge conflicts

The taskbar entries are stored in a hidden folder. The location of the hidden folder (on Windows 8) is as follows: C:\Users\{username}\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar

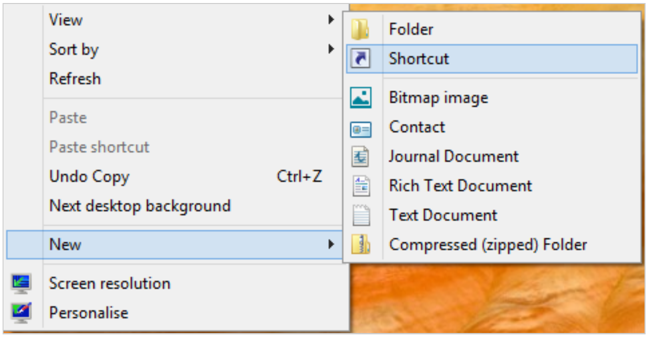


Name	Date modified	Type	Size
Google Chrome	6/8/2014 11:11 AM	Shortcut	3 KB
iexplore	11/9/2013 11:27 AM	Shortcut	2 KB
Mozilla Firefox	11/9/2013 11:46 AM	Shortcut	2 KB
Opera	9/24/2014 3:20 PM	Shortcut	2 KB



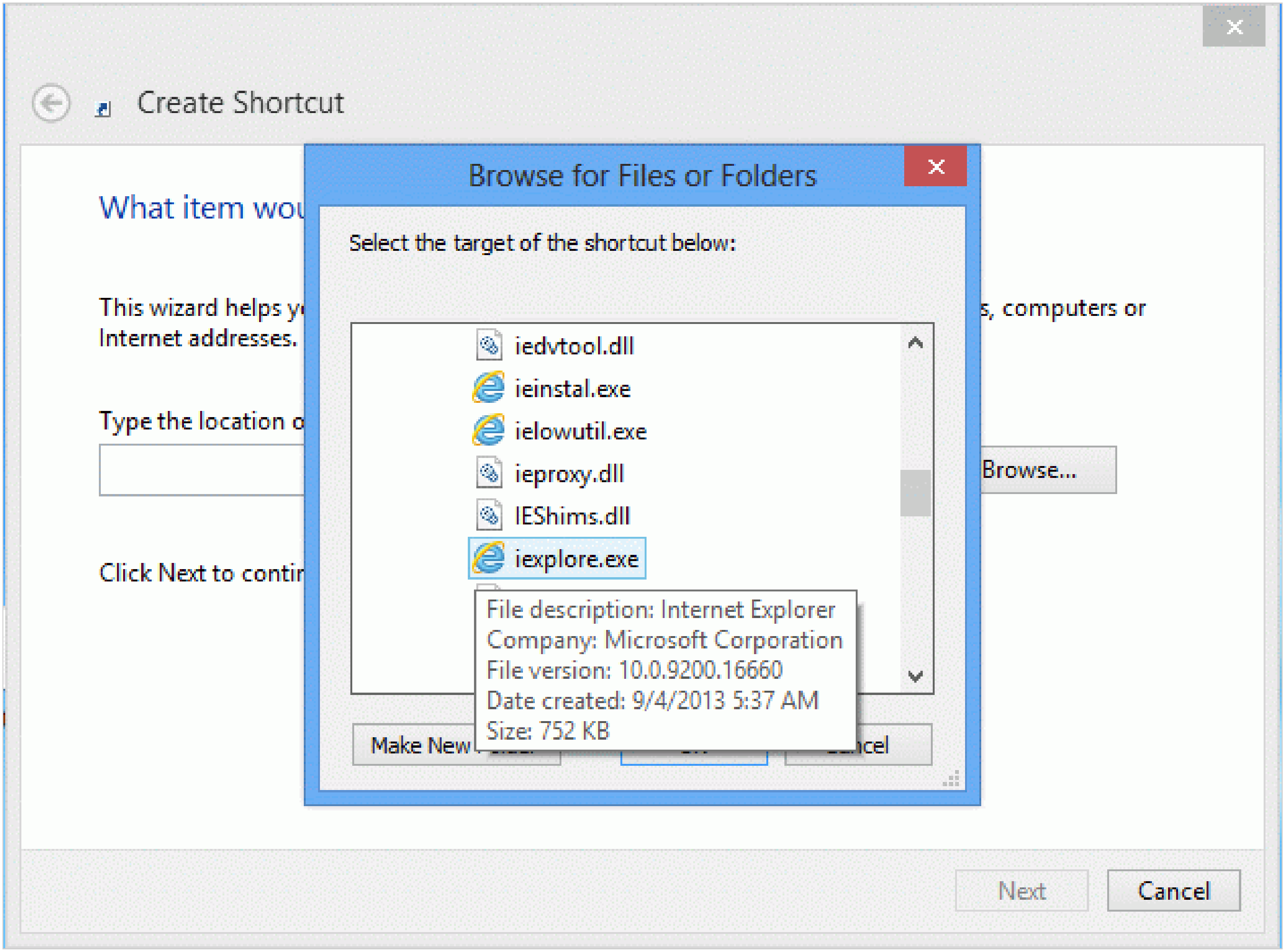
Select the shortcuts you'd like to remove and delete them. (Or right-click and delete.) Removing shortcuts from this location may require a reboot for the removal to take effect.

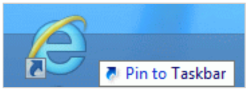
Once the altered shortcut is removed, right-click your desktop and choose "New" then "Shortcut."



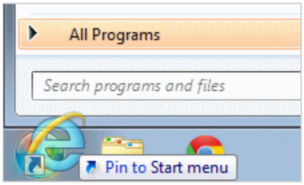
Then browse to the location of the program you want to start with the shortcut.
Common locations for browsers are:
"C:\Program Files\Internet Explorer\iexplore.exe"
"C:\Program Files\Google\Chrome\Application\chrome.exe"
"C:\Program Files\Mozilla Firefox\firefox.exe"
"C:\Program Files\Opera\launcher.exe"

"Program Files" may be "Program Files (x86)" if you are running a 64-bit operating system.
Please note that the quotes are necessary for these shortcuts to work.

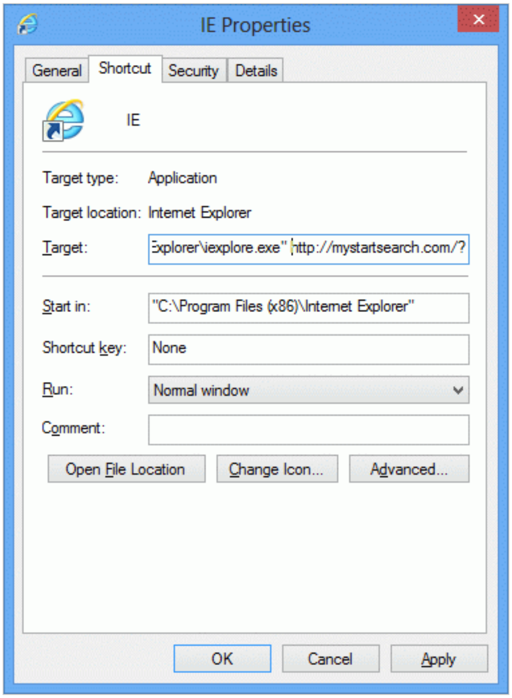




You can use the same procedure to pin the shortcut to the Start menu by dragging the icon to the start button.



Existing shortcuts on the desktop can also be cleaned by right-clicking them, then choosing "Properties." In the "Target" field, remove everything after the path to the program. Remember to leave the quotes.



IE

Target type: Application

Target location: Internet Explorer

Target: Explorer\iexplore.exe" http://mystartsearch.com/?

Start in: "C:\Program Files (x86)\Internet Explorer"

Shortcut key: None

Run: Normal window

Comment:

NEWSLETTER

Enter your e-mail

SUBMIT

CONTACT

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

EULA Privacy Terms of Service

Malwarebytes