

# 8 ways to prevent websites from automatically opening in Chrome

By opening unwanted web pages in new tabs, Chrome often frustrates users. Hidden malware could be the cause, but the problem could also be in your browser settings itself.

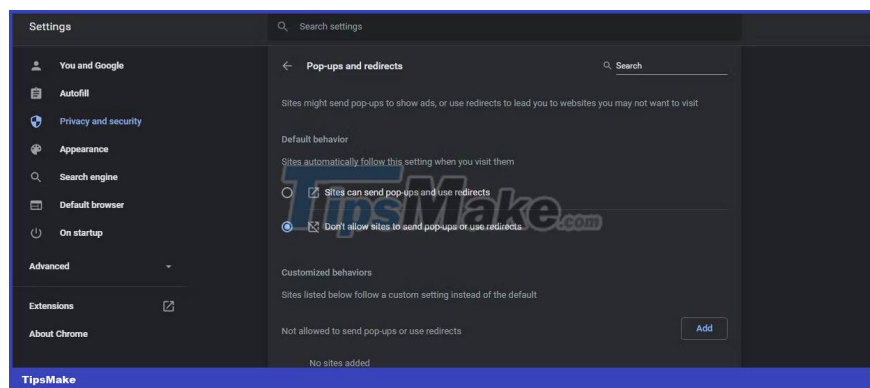
Take a look at 8 different ways to prevent unwanted websites from opening in Chrome.

## 1. Block pop-ups and redirects

Using redirects, websites can send traffic to their desired location. It could be an affiliate page, a landing page, or a promotion. As a result, you will be redirected to multiple pages every time you visit such a website. It can also cause unwanted web pages and pop-ups to open.

Fortunately, Chrome allows you to block that activity by disabling the setting that allows websites to use pop-ups and redirects. To do so, follow these steps:

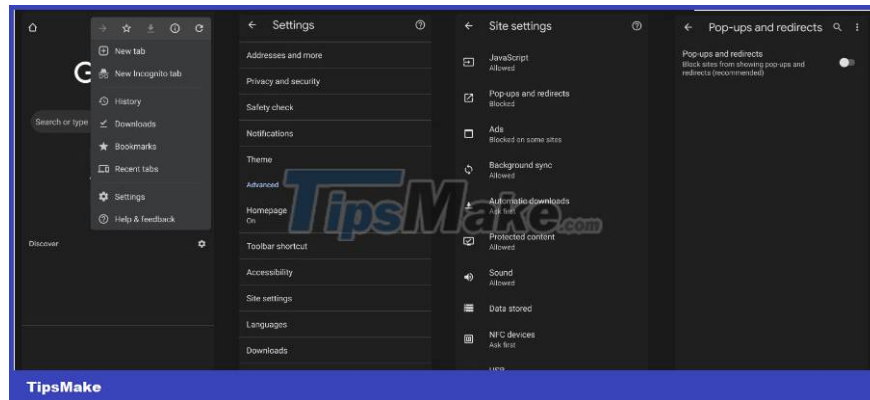
1. Click the three vertical dots in the top right corner to access **Settings** .
2. **In the left sidebar, click Privacy and Security settings** .
3. Click **Site Settings** and scroll down to **Content** settings .
4. Click **Pop-ups and redirects** .
5. Select **Don't allow sites to send pop-ups or use redirects** .



Then scroll down to **Customized behaviors** and remove all sites from the **Allowed to send pop-ups and use redirects** section . Avoid adding new sites in the future.

To block pop-ups and redirects in Chrome on Android, follow these steps:

1. Launch Chrome.
2. Tap the three vertical dots in the upper right corner and select **Settings** .
3. Go to **Site settings > Pop-ups and redirects** .
4. Turn off the toggle next to **Pop-ups and redirects** .



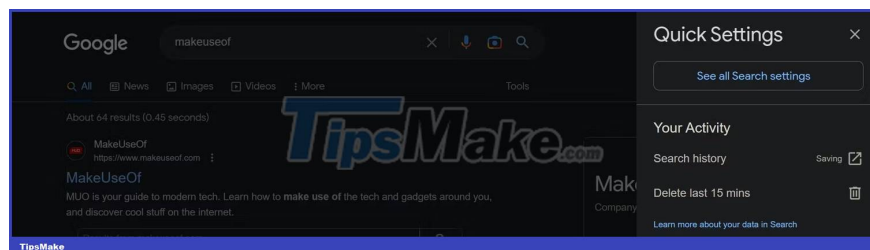
## 2. Change search settings in Chrome

You can prevent Chrome from opening unwanted web pages at the same time by adjusting your search settings. While it may not solve the whole problem, it does allow you to control how many unwanted websites are open at once.

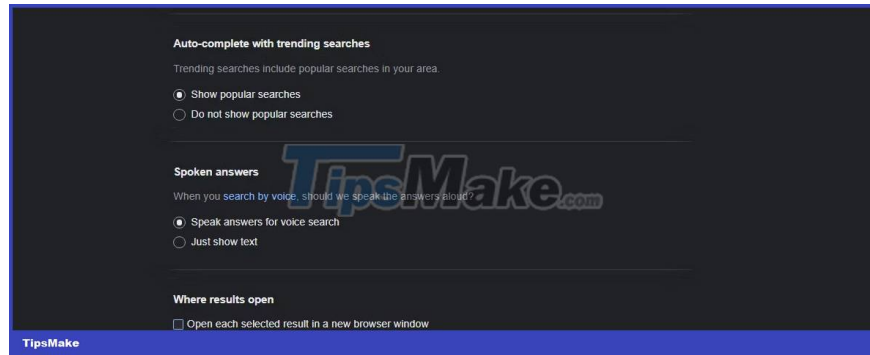
By default, Chrome opens any new pop-ups or web pages in a new tab. Every time a new unwanted website opens in Chrome, it opens in a new tab. This allows viruses and bugs to freely redirect you to different pages at the same time.

You can effectively restrict Chrome from opening web pages in new tabs. Then all new web pages will open in the same tab.

To do that, go to the Chrome search bar and search for anything. Click the **Settings** icon in the top right and click **See all Search settings** .



Scroll to the bottom of the search settings page and uncheck the box **Open each selected result in a new browser window** .

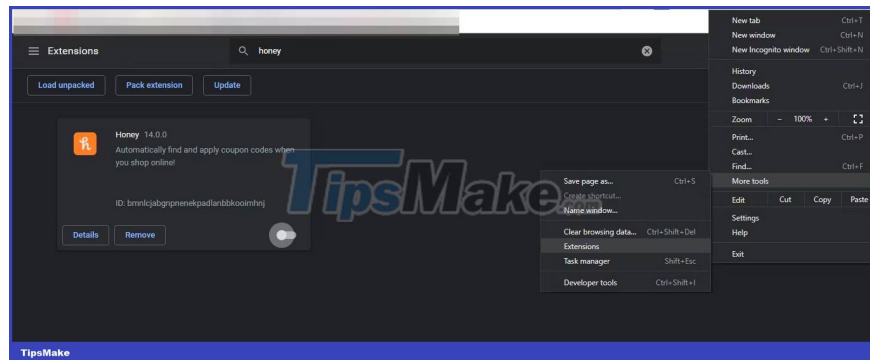


Therefore, if the problem occurs along with anything else, it can also disrupt your browsing by opening unwanted websites that replace the one you clicked to visit. In that case, undo the change.

### 3. Disable Shopping Extensions

If you are only redirected to specific pages, such as a shopping site, then you may be using a money-saving or coupon shopping extension. Coupon extensions work by finding the most relevant coupon for your purchase and can redirect you to another website or another page of the same website.

This can lead to many unwanted web pages being opened within seconds. Consider disabling all coupon and discount extensions you're using to make sure that doesn't happen. You can disable extensions in Chrome by clicking the three vertical dots in the top right corner and navigating to **More Tools > Extensions** .



If disabling the coupon extension doesn't yield any results, disable the ad blocker extension in Chrome.

### 4. Remove the ad-blocking extension

The ad blocker extension prevents visited pages from being flooded with ads. While very useful, it also has its downsides. By filtering content, ad blockers prevent specific content from appearing on websites, directly interfering with website scripts.

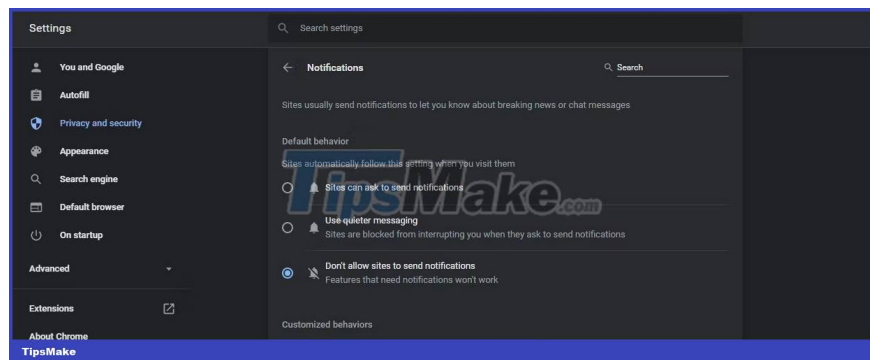
Such interference can also lead to unusual problems such as the one under discussion. To determine if the problem is caused by ad blocking, disable them and see if the problem persists. If so, proceed with the remaining fixes.

## 5. Block Website Notifications

Whenever you visit a new website, you will be asked for permission to receive notifications from that website. By accident, you may have turned on notifications on websites that offer an unsecured connection. These sites may redirect you to unwanted websites when you tap on their notifications.

Here's how you can rule this out by turning off notifications:

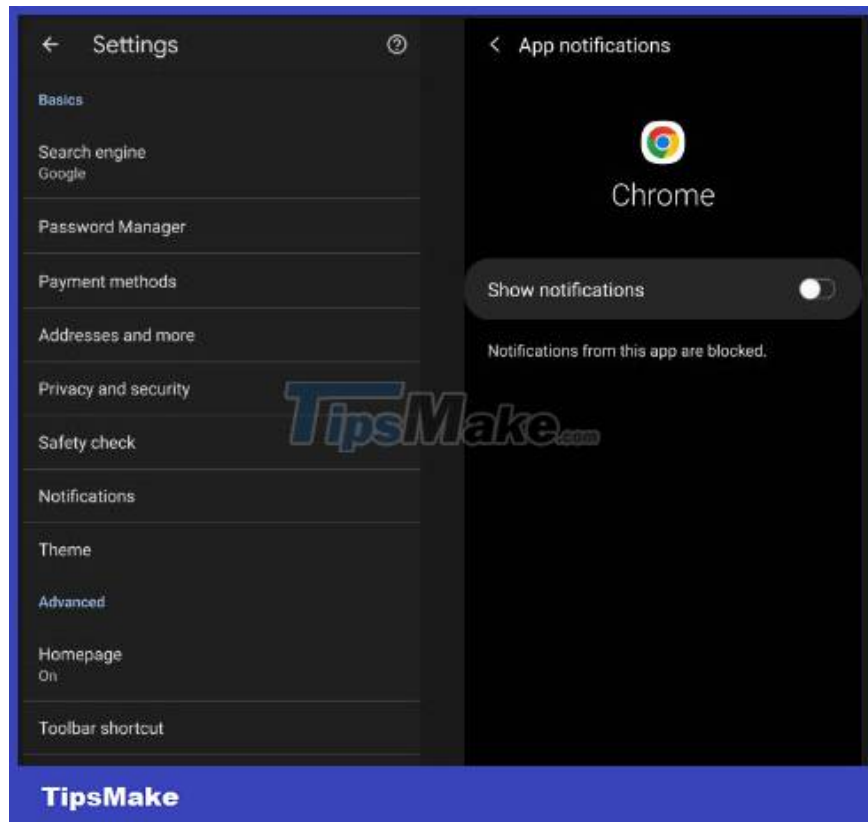
1. Go to Chrome's settings.
2. **On the left sidebar, click Privacy and security settings .**
3. Go to **Site Settings** .
4. Go to the **Notifications** section under **Permissions** .
5. Select **Don't allow sites to send notifications** .



**Then, scroll down and remove any suspicious websites from the list of Allowed to send notifications websites . Remove them all to avoid further distractions.**

To turn off notifications in Chrome on Android, follow these steps:

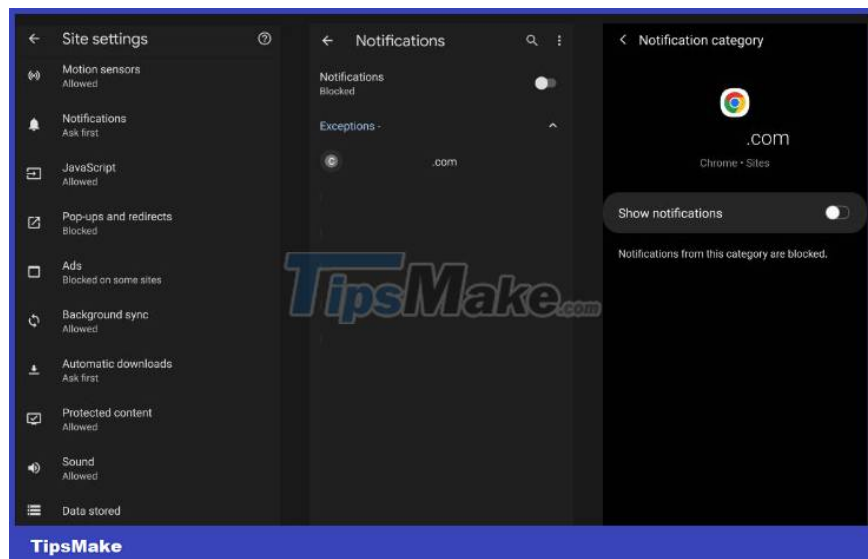
1. Launch Chrome.
2. Tap the three vertical dots in the upper right corner and select **Settings** .
3. Go to the **Notifications** section .
4. Turn off the toggle next to **Show notifications** .



5. Return to the **Settings** page again.

6. Navigate to **Site settings > Notifications** .

7. Turn off the toggle next to **Notifications** .



If some suspicious websites appear in the **Exceptions** list , tap each website one by one and turn off the toggle next to **Show notifications** for each site separately.

## 6. Search for browser hijacker

Browser hijacker is a piece of malware that targets web browsers and infects them with viruses. Once in the browser, the hijacker will change its settings, change the default search engine (in most cases to Yahoo), change the default homepage, track user activity, etc. The Hijacker does all of this without the user's consent or knowledge.

In addition to compromising security, the hijacker also changes browser settings and can automatically redirect you to unwanted websites. If your browser automatically opens random websites, it may have been hacked. Therefore, it is imperative to rule out this possibility.

To make sure your browser isn't compromised, check to make sure that no suspicious extensions have been added, no shady search engines have been selected as default, and that the hijacker hasn't changed. change the default browser settings. Look for suspicious changes in the browser and revert them.

Be careful when installing third-party applications in the future, as the hijacker often comes with untrusted software. This way, you can protect your device from being compromised.

## 7. Clear cookies and cache

If Chrome is still opening unwanted web pages, you can clear Chrome's cookies and cache to eliminate the possibility of harmful cached data.

Refer to the guide: [How to clear cache and cookies on Chrome, Firefox, Coc Coc and Safari](#) for details.

## 8. Reset or reinstall Chrome

After all other fixes have been applied, update Chrome to the latest version to see if it fixes the problem. In case this doesn't work, you can try resetting Chrome or reinstalling the browser. However, there is a downside to both methods.

Reset or reinstall Chrome means restarting Chrome, reverting all changes to defaults, and deleting all your account information unless you've synced it before.

Remember that clearing app data will erase all your customizations and reset settings to defaults. Next time you open Chrome, it will look like the browser just installed. So you'll need to log into your account and customize the browser from scratch.

If resetting Chrome doesn't solve the problem, you can reinstall the browser.

You finished reading the article "**8 ways to prevent websites from automatically opening in Chrome**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.