

This article will tell you how to clear cookies and cache on your browser, computer, or phone. Cookies are small files that are automatically created by the websites we visit. They are stored on your device to ensure you have a seamless user experience. Cache stores data locally so it can be loaded faster.

Cookies facilitate various functions on websites. They are usually added to your computer after you enter a site or after a specific interaction, and they typically expire after some time. In the meantime, cache accumulates much more data on your computer which can significantly reduce free disk space.

With that said, **it's good practice, both in terms of privacy and performance, to periodically clear cookies and cache.**

Different platforms have their own way of clearing cache and cookies. For that reason, we offer you step-by-step guides on how to delete browser cookies and cache on all devices and browsers.

[1. Clear cookies on your browser](#)

- [How to clear cookies on Chrome](#)
- [How to clear cookies on Firefox](#)
- [How to clear cookies on Microsoft Edge](#)
- [How to clear cookies on Safari](#)

[2. Clear cookies and cache from your computer and phone](#)

- [How to clear cache on Mac](#)
- [How to clear cache and cookies on Windows](#)
- [How to clear cache and cookies on iPhone](#)
- [How to clear cookies and cache on Android](#)
- [How to clear cookies on iPad](#)

[3. Should you accept cookies or not?](#)

[4. How often should you clear cookies](#)

[5. Reasons to clear cookies](#)

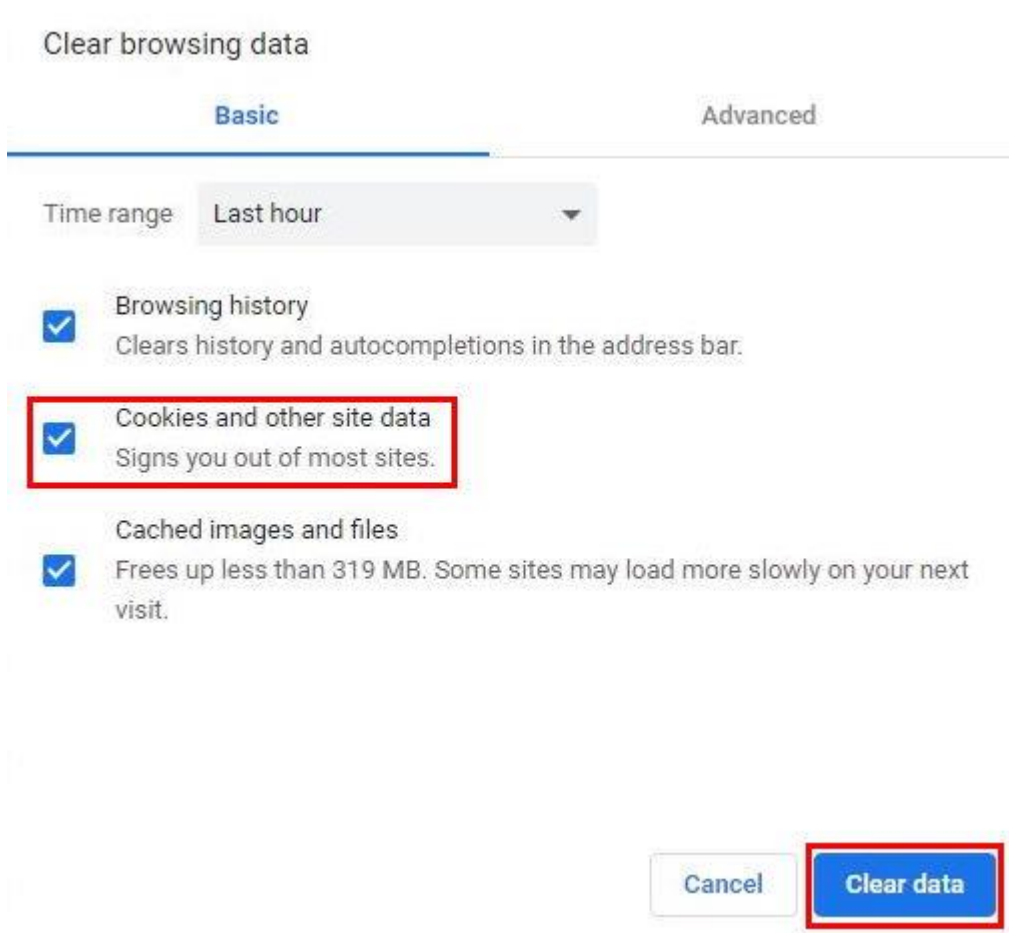
[6. Cookie types](#)

[7. Wrapping up](#)

Clearing cookies on Chrome, Firefox, Microsoft Edge and Safari

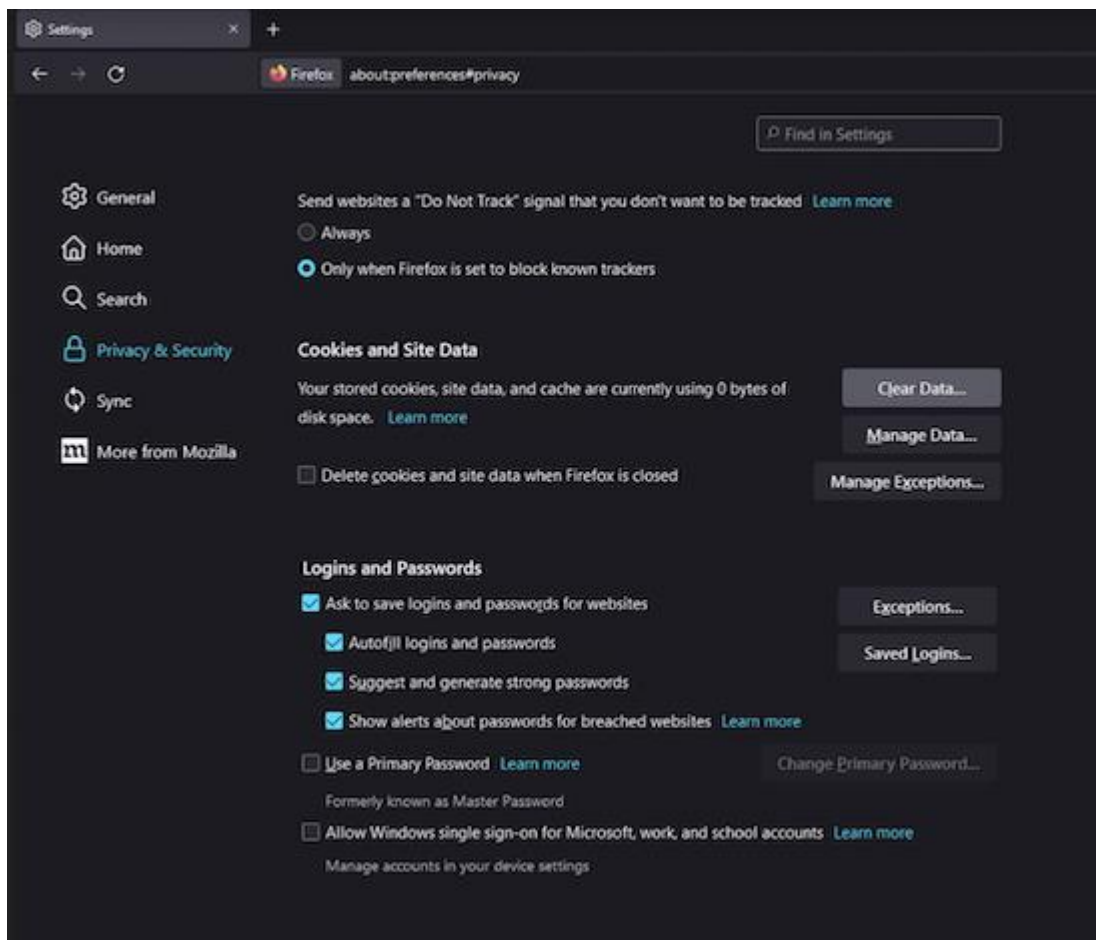
Clear cookies on Chrome

1. Navigate to the top right corner and click the **icon with three upright dots**, which lead to Customize and control Google Chrome menu
2. Hover over **More tools** and select **Clear browsing data**
3. Leave only **Cookies and other site data** ticked if you don't want to clear history or cache
4. Select a **Time range** from the drop-down. We recommend **All time**
5. Click **Clear data** to delete all cookies on Chrome



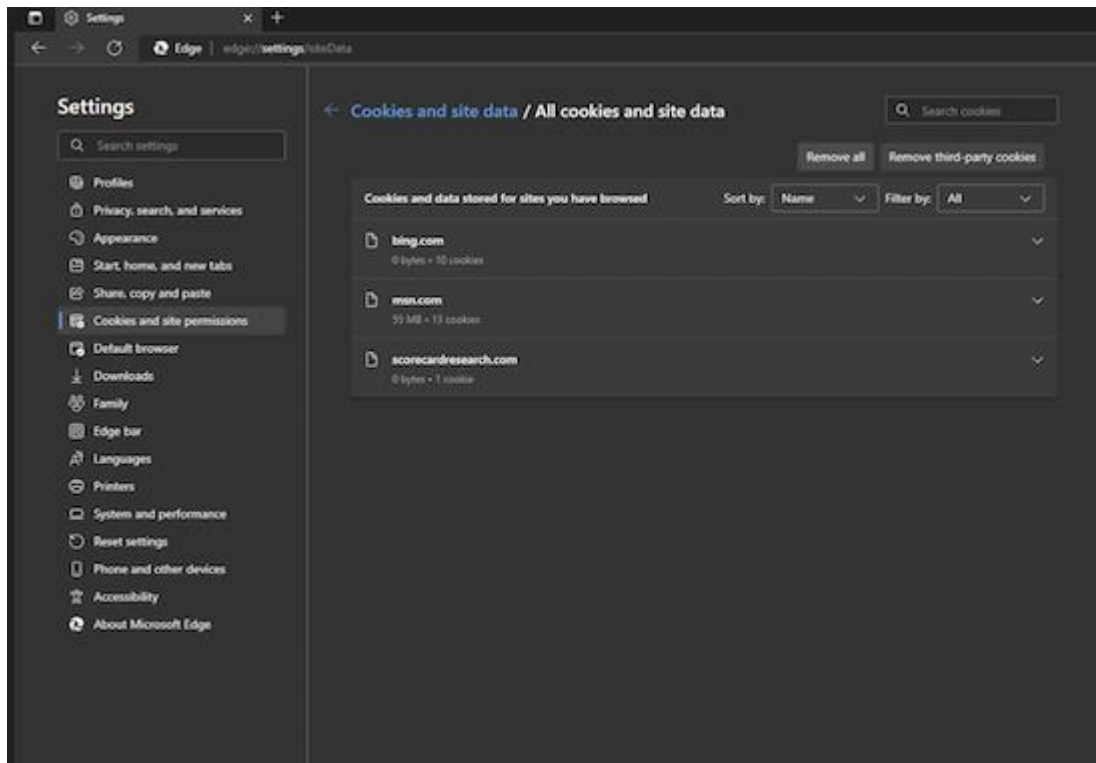
Clear cookies on Firefox

1. Click on the **menu icon** (☰) located on the top right corner of your Firefox browser
2. From the drop-down menu, select **Settings**
3. Click on **Privacy and security** that is found on the left hand side
4. Scroll down to **Cookies and Site Data** menu
5. Select to **clear data**
6. **Choose** what do you wish to remove and **clear it**
7. Tap **Clear now**, and you're all set



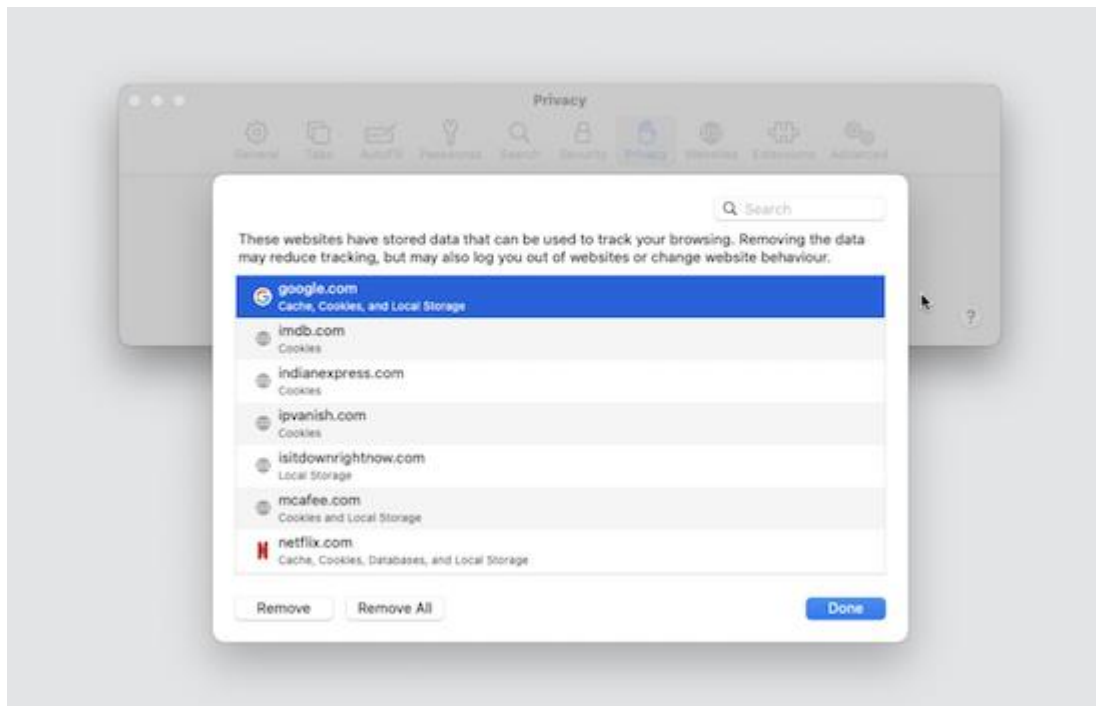
Clear cookies on Microsoft Edge

1. On the top-right, click the **three dots** which represent **Settings**
2. On the left hand side locate **Cookies and site permissions** and choose it
3. Click on **Manage and delete cookies and site data**
4. Go to **See all cookies and site data**
5. Choose what you wish to clear or **Remove all**



Clear cookies on Safari

1. Choose **Safari** and then **Preferences**
2. Click **Privacy**
3. Choose **Manage Website Data**
4. Optionally, select the websites that you want to stay with cookies and **Remove** others manually
5. Click **Remove All** to delete all cookies
6. Once you're finished, click the blue **Done** button



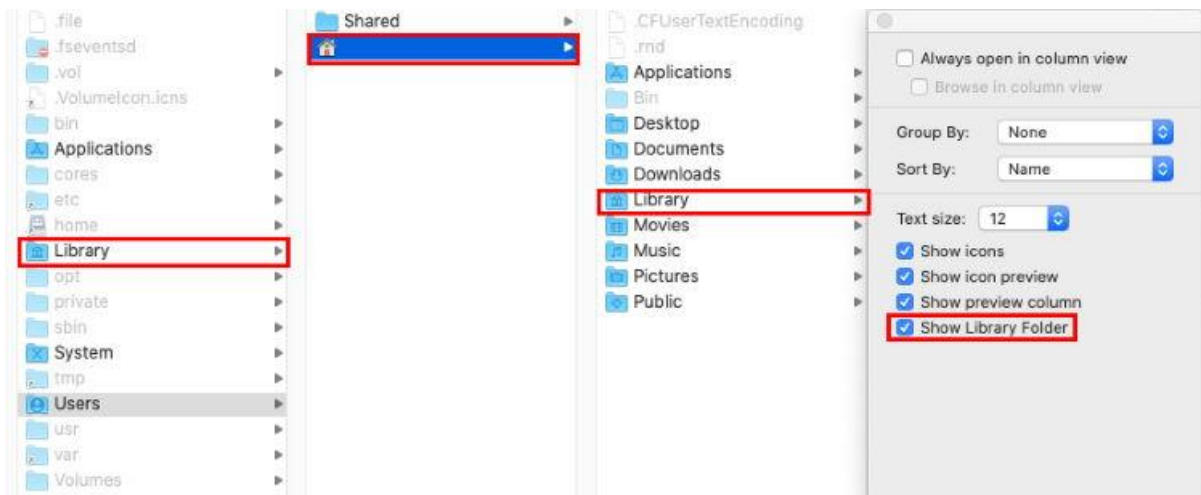
Clear cookies and cache from your computer and phone

Clear cache on Mac

Like all computers, Macs store cache on their hard drives. The more apps you install and the more you use them, the bigger your cache will be. It's not uncommon to find it exceeding 10 GB or even more.

Here is a step by step guide on how to clear cache on Mac:

1. Locate the **Library** folder on your Mac
2. Go to the **Cache** subfolder and **delete everything inside**. Don't delete the folder itself
3. Launch **Finder** and open **Users/your_username**
4. Choose **View** and then **Show View Options**
5. Select **Show Library Folder** and close the window
6. Locate the now visible **~Library** folder
7. Go to the **Cache** subfolder and **delete everything inside**. Don't delete the folder itself



Note that deleting cache for specific apps will clear your settings. You may also need to log in again to the websites that you use. However, once you do that, the services will recapture and save your account details.

Clear cache and cookies on Windows

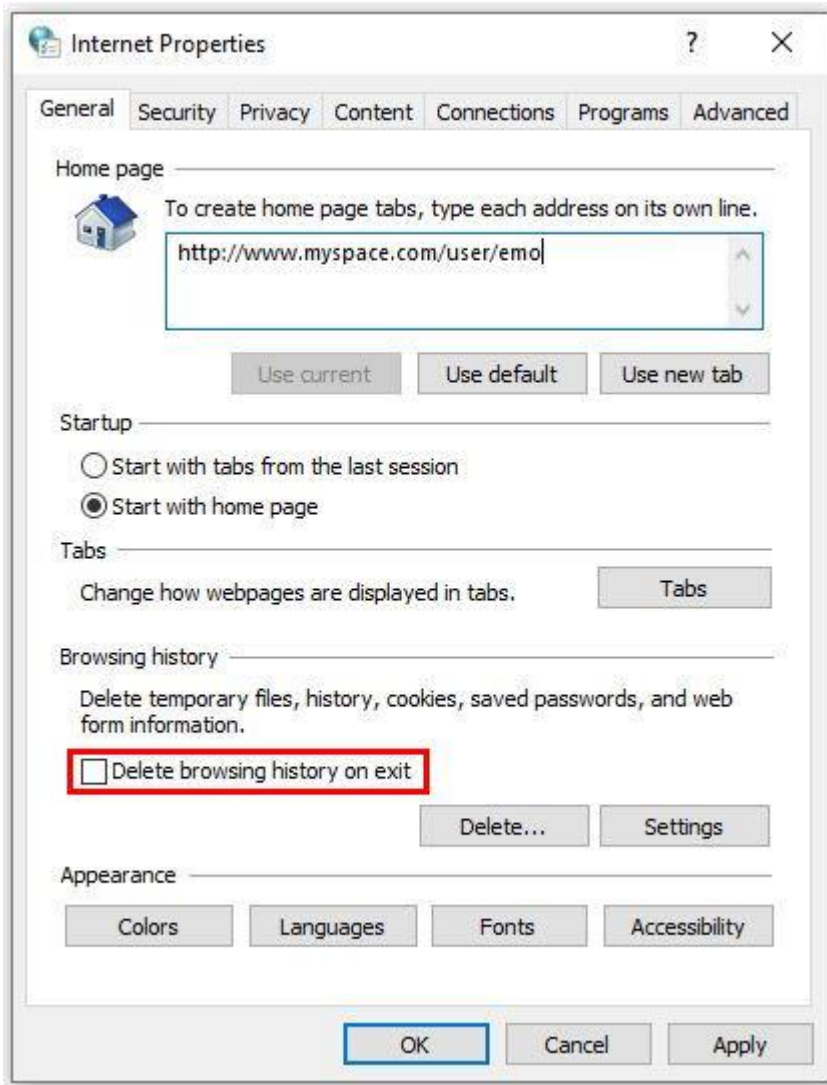
The process of how to delete browser cookies and cache on Windows 10 and Windows 11 is similar to that of Windows 7. However, there is a major difference in where to locate the necessary settings required to access the "delete" option.

Clear cookies on Windows 10 and Windows 11

There are two ways to delete cookies on Windows 10 and Windows 11.

Option 1: Deleting browser cookies in Internet Explorer on Windows 10 and Windows 11

1. Open the Internet Explorer and click on the **Tools cogwheel** at the top right
2. A drop-down menu will appear. Hover over **Safety**
3. Select **Delete browsing history**
4. Leave only **Cookies and website data** ticked, if you want to keep other data
5. Hit **Delete**



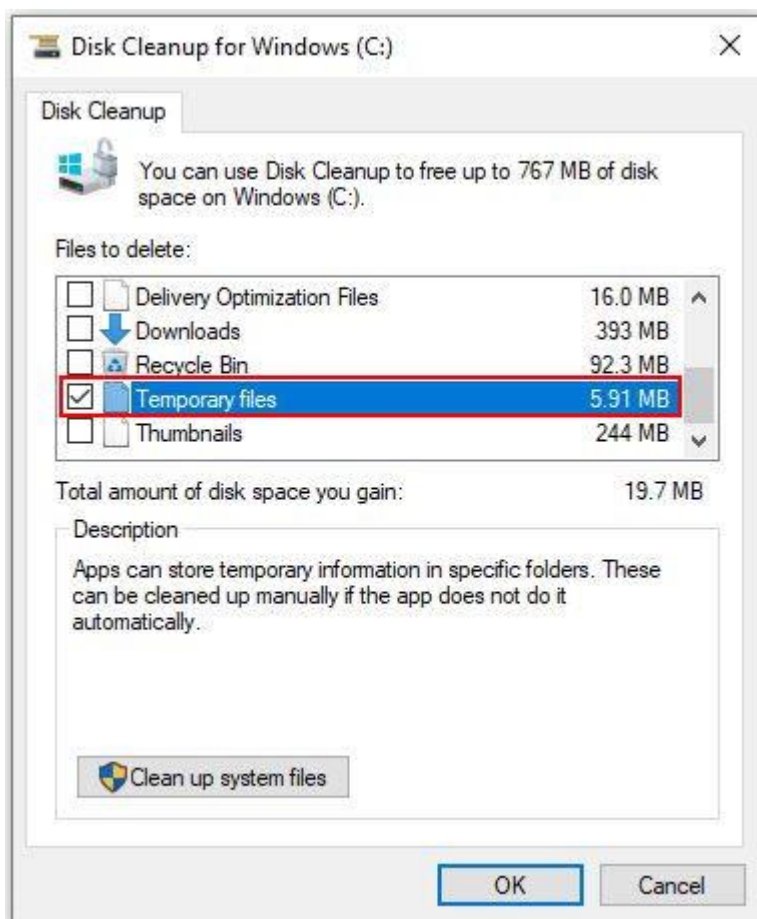
Option 2: Deleting browser cookies in Windows 10 and Windows 11

1. Hit the **Windows** button and search for the **Control Panel** app
2. Open **Network and Internet**
3. Under **Internet Options**, choose **Delete browsing history and cookies**
4. Under **Browsing history**, choose **Delete browsing history on exit** and hit **OK**
5. If you want to delete cookies only, hit **Delete...** button and untick other boxes

The only difference on Windows 11 is that we won't see a **Delete browsing history on exit** tickable box. Also, only **Browsing history** and **Appearance** settings are included in the General tab.

Clear cache on Windows 10 and Windows 11

1. Press the **Windows key** and lookup **Disk Cleanup**
2. Select the drive you want to clean up. Most likely it will be **C:**
3. Scroll down the list and tick **Temporary files** to clean cache
4. Optionally, delete Thumbnails, Downloads, and other data you may not need
5. Optionally, click the **Clean up system files** button to calculate how much the downloaded updates take-up
6. Click **OK**



Clear cookies on Windows 7

Option 1: Delete browser cookies in Internet Explorer 7

1. Click **Tools** at the top right of your Internet Explorer 7 window
2. From the dropdown, select **Internet Options**
3. In the **General** tab, click the **Delete...** button under **Browsing history**

4. Click **Delete cookies** and confirm by pressing **Yes**
5. Optionally, you can also delete temporary internet files, browsing history, form data, and passwords

Option 2: Delete browser cookies in Windows 7

1. Click the **Start** button
2. Type **Internet Options** and click it
3. Under the **General** tab, click **Settings**
4. Click **View files** at the bottom-right corner
5. Select all files with **Ctrl + A**
6. Delete all files with **Shift + Del**

Clear cache on Windows 7

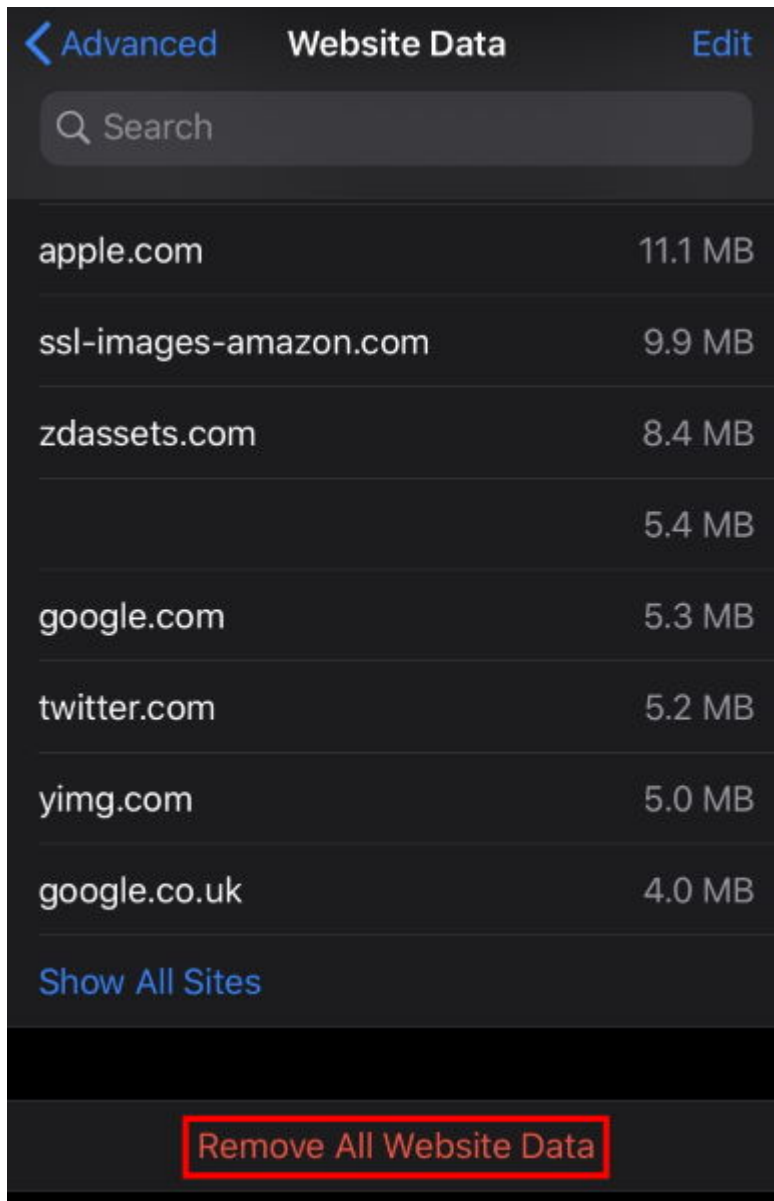
1. Click the **Start** button
2. Type **Disk Cleanup** and click it
3. Select the drive you want to clean up. Most likely it will be **C:**
4. Check the box that says **Temporary files**
5. Optionally, check other boxes as well
6. Click **Delete Files**. The window will close automatically

Clear cache and cookies on iPhone

Clear cookies on iPhone

Here's how to clear Safari cookies on an iPhone:

1. Pay a visit to **Settings**
2. Scroll down until you find **Safari**. Tap it!
3. Scroll all the way down until you reach **Advanced**. Tap it!
4. Choose **Website Data**
5. Select **Remove All Website Data** or **Edit** to select cookies of each website manually
6. If you want to delete browser history together with cookies, get back to **Safari** and tap **Clear History and Website Data**

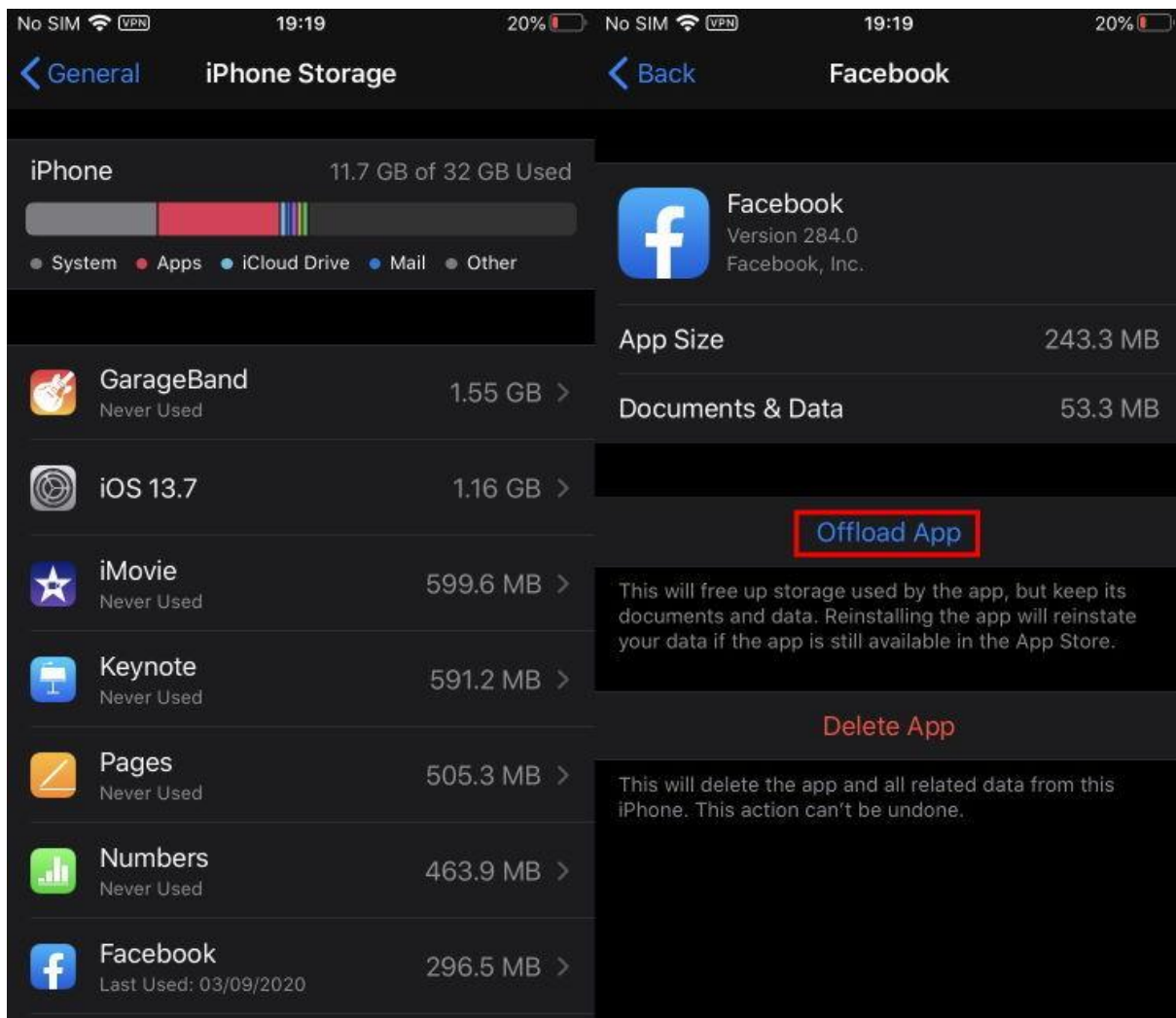


Clear cache on iPhone

There's no universal method for clearing cache on iPhone. Instead, you can review separate apps and remove data that you no longer need. Some of them will have simple "Clear cache" options but others will require more of your attention and patience.

To clear cache on your iPhone:

1. Go to **Settings** and tap **General**
2. Choose **iPhone Storage**
3. From the list, choose an app that takes a significant amount of space
4. If you're running out of space, you will see **Recommendations** for a cleanup
5. If you have enough space, you can choose **Offload App** to keep the data but remove the app itself

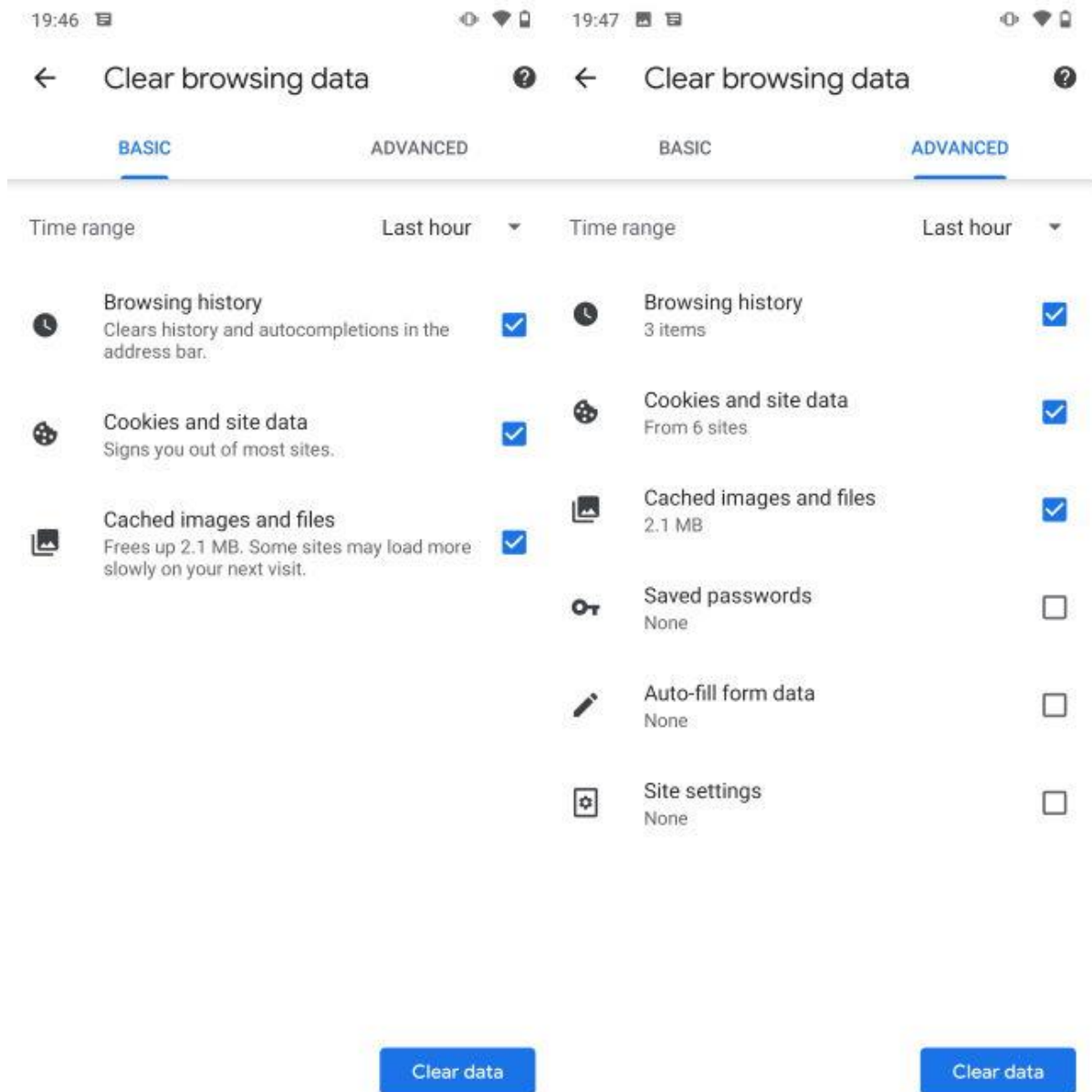


Clear cookies and cache on Android

Clear cookies on Android

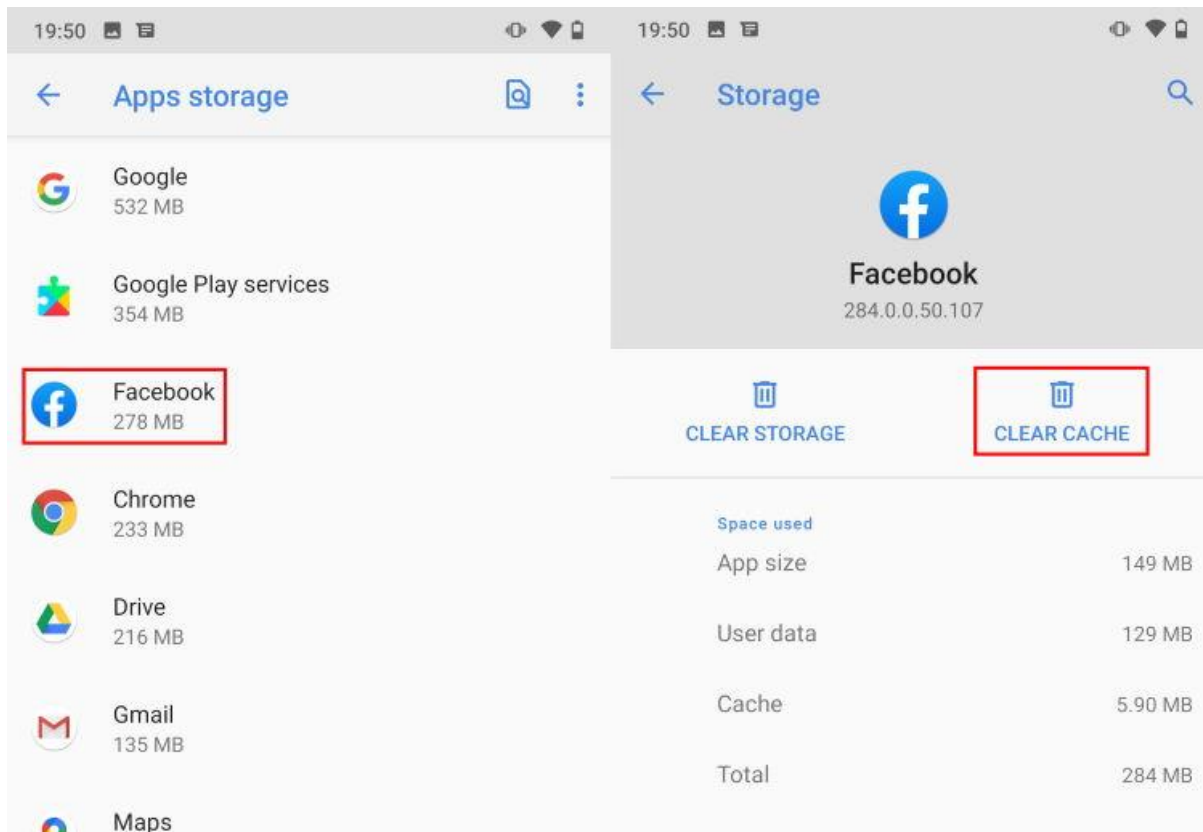
The following guide is written for Chrome users. If you want to delete cookies from another browser, please refer to their support.

1. Open the Chrome browser and tap the **three dots (More)** at the top right
2. Select **History**
3. Choose **Clear browsing data**
4. Select a **Time range**. We recommend **All time**
5. If you want to delete cookies only, deselect **Browsing history** and **Cached images and files**
6. If you also want to delete passwords, autofill, and site settings, go to the **Advanced** tab
7. Tap the blue **Clear data** button



Clear cache on Android

1. Go to **Settings**
2. Tap **Storage**
3. Select **Other apps**
4. Choose the app – there's no way to remove the cache of all apps at once
5. Tap **Clear cache**



How to clear cookies on iPad

Note that clearing cookies on iPad won't log you out of all websites. This information is controlled by AutoFill.

Here is how to clear cookies on iPad:

1. Go to **Settings** and choose **Safari**
2. Tap **Advanced** at the very bottom and then **Website Data**
3. Select **Remove All Website Data**
4. If you want to clear your history as well, tap **Clear History and Website Data** under **Safari**

If there are no cookies or browsing history to clear, the setting will fade to grey.

Should you accept cookies or not?

Sometimes it makes sense to keep cookies enabled. There's no denying that they make things easier by, for example, removing the need to remember passwords, especially for your regularly visited sites.

As mentioned previously, **cookies also increase the relevance of content you see online** because they help services track what you're interested in.

With that said, **almost every type of cookie reduces your privacy** by a little bit – some more, some less. Therefore, disabling them is a very valid consideration. If you don't want to do that, at least clean your cookies on a regular basis.

How often should you clear cookies

In the era of diminishing privacy, clearing cookies is a good idea and this is not so hard to illustrate by example. In 2015-2016, hackers breached Yahoo's systems, stealing proprietary codes related to the cookies of around 32 million users. This gave the attackers the ability to forge cookies and thus gain access to millions of accounts.

And this is just one example – by **allowing cookies to remain on your computer for a long time, you are giving advertisers and data mining companies the green light** to track your online activities. This certainly doesn't increase your privacy.

So how often should you clean these cookies? If you're using a public computer, you should delete them and other data, such as browsing history, right after your session. If it's your personal device, **it's a good idea to remove all cookies at least once a month to keep your device neat**. Also, you should do this if you see a drop in browser performance or after visiting a shady website. This will make you re-enter multiple logins, but doing that for the sake of your privacy is worth it.

Reasons to clear cookies

As almost any expert will tell you, few things are black or white when it comes to technology – it's all about how you use it. The choice to enable or disable cookies is a maths problem of weighing convenience against privacy and, in some senses, performance. That being said, there are some really good reasons to clear your cookies regularly:

- **Increased security risk.** Cookies can be hijacked by hackers that want to access your browser session data.
- **Decreased performance.** Cookies tend to slow your browser down. While they make websites load faster at first by storing some of the info on your device, cookies start clogging things up after some time.
- **Increased privacy risk.** Your personal data stays in the cookies and adds up as you surf the web. This results in more personalized ads and more data that can be sold to third-parties. Also, the more private information your cookies contain, the easier it is for a hacker to use it against you.
- **Account protection.** If someone takes over your device, he or she will be able to use services under your name without logging in.

What do cookies do?

A cookie is a piece of data stored on your device by your browser. Their purpose is to **remember your actions**, such as the items in your shopping cart, and **your data**,

such as passwords or credit cards. Cookies also **collect information about your online behavior**. This can include the buttons you've clicked or the pages you've visited.

There are different types of cookies, discussed in the section below. Some let a server know whether you're still logged so that it doesn't send sensitive information when it shouldn't. Others recognize your personal preferences, such as site language. Finally, the so-called zombie cookies are borderline malware because they re-appear the moment you delete them and are built for aggressive tracking. On the other hand, they may help site owners to block unwanted traffic.

Cookie types

Session cookies

Short-term cookies like these remain on your computer until you close your browser. An example of their use is by e-commerce websites, allowing you to use online shopping carts effectively. Another example is a cookie that makes your browser's "Back" button work so that you don't get a fresh copy of that page without your input.

Persistent cookies

This term refers to those cookies that stay on your device from session to session. In other words, they don't self-erase after you close your browser. An example of such cookies is those that store your login credentials. Legally, most countries require these cookies to expire after a certain period of time, which can often mean months.

Tracking is another purpose for using persistent cookies. They track your visits over the period of time and build up your profile. It can later be used to customize your experience on a specific website.

Third party cookies

These are the most dangerous cookies due to privacy reasons because they are added to your device by third-parties operating on a website you visit. They collect information about you in ways described within the Privacy Policy documents of these services. Some sites will have more than 50 such cookies, making the task of ensuring your privacy impossible.

You can minimize your exposure to these third-party trackers by using browser extensions like Ghostery. Another option is to block cookies completely, although this would mean that you'll have to enter your login details every time you visit your favorite online services.

Wrapping up

It's important to know what you're up against when it comes to cookies. Consider how much privacy you're willing to give up for the sake of convenience and act accordingly. And, regardless of the situation – be sure to clear them occasionally, especially after you visit some dubious sites.

Another tip is to browse using a private mode that doesn't store any information. Of course, you will probably not want to use it all the time. That's because you'll have to enter login details to Gmail, Facebook, and other services after each session. Therefore, for most users, the right path will be somewhere between all cookies and no cookies at all.