THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

January 2024

Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

This month, we are observing Data Privacy Day/Week, which begins on January 21st and culminates on January 28th. This global initiative aims to raise awareness about the significance of data privacy and to ensure that individuals are equipped with the knowledge to protect their data. While January 28th is internationally recognized as Data Privacy Day, organizations such as the National Cyber Security Alliance believe that a single day is insufficient. As a result, an entire week is dedicated to educating people on this subject. The theme for this year is "TAKE CONTROL OF YOUR DATA."

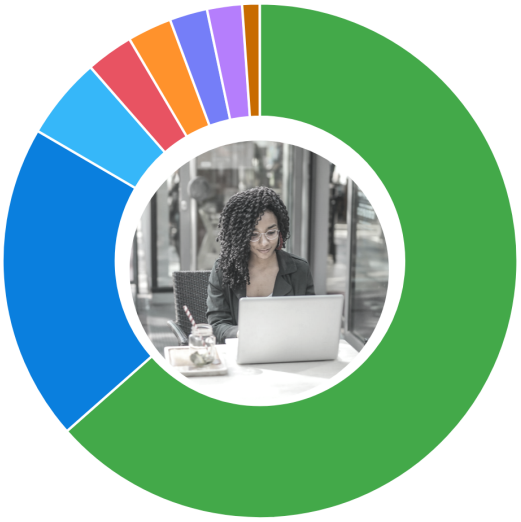
In this edition, I will be discussing browsers and how to adjust your browser privacy settings from the 3 most popular web browsers to help you stay safe in the cyber world.

What are the worlds most popular web browsers?

According to Venngage.com, in 2023 the most popular browsers are Chrome, followed by Mac Safari and Microsoft Edge. By popularity, statista.com also found that Chrome, followed by Mac Safari and Microsoft Edge where the most widely used. Other sites also agree on the top 3, but rankings for 4th and below are often a source of much debate.

Most Popular Web Browsers in 2023

Most people choose a web browser based on speed, security, compatibility, simplicity, appearance, and/or popularity. But sometimes people stick with a browser just because it came installed and are not aware of other options.



Chrome
Safari
Edge
Opera
Fixefox
Samsung Internet
Others
UC Browser

Google Chrome **63.55%**

Mac Safari **19.95%**

Microsoft Edge **5.14%**

Opera **2.98%**

Mozilla Fixefox **2.79%**

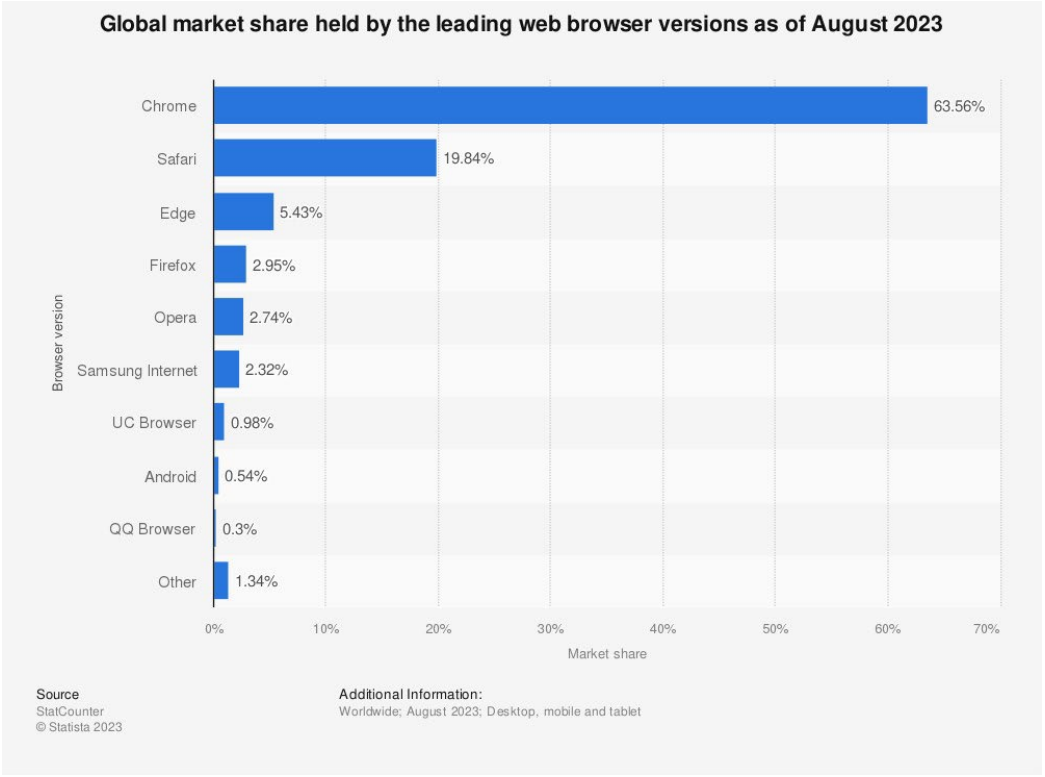
Samsung Internet **2.38%**

Others **2.2%**

UC Browser **1.1%**

VENNGAGE

Source: StatCounter I Data collected on July 2023



Google Chrome features and tools

This popular browser includes numerous features and tools for browsing, such as:

- Add-ons and web extensions.
- Dark mode.
- Data breaches warning.
- Forms autofill.
- Multiple profiles.
- Password management.
- Picture-in-picture.
- Private mode.
- Reader mode.
- Spell checking.
- Strong password generation.
- Sync across multiple devices.
- Tab browsing.
- Tab groups.
- Text to speech.

Developer: Google LLC.

Supported operating systems: Android, Chrome OS, iOS, Linux, MacOS and Windows.

License: proprietary freeware.

Safari features and tools

This popular browser includes numerous features and tools for browsing, such as:

- Add-ons and web extensions.
- Dark mode.
- Data breaches warning.
- Forms autofill.
- Password management.
- Picture-in-picture.
- Private mode.
- Quick notes.
- Reader mode.
- Spell checking.
- Strong password generation.
- Sync across multiple devices.
- Tab browsing.
- Tab groups.
- Text to speech.
- Third-party cookies and social trackers blocked.
- 4K video streaming.

Developer: Apple Inc.

Supported operating systems: iOS, iPadOS and MacOS.

License: freeware and GNU LGPL for some components.

Microsoft Edge features and tools

This popular browser includes numerous features and tools for browsing, such as:

- Add-ons and web extensions.
- Dark mode.
- Data breaches warning.
- Forms autofill.
- Kids browsing mode.
- Multiple profiles.
- Password management.
- Picture-in-picture.
- Private mode.
- Reader mode.
- Spell checking.
- Strong password generation.
- Sync across multiple devices.
- Tab browsing.
- Tab groups.
- Text to speech.
- Third-party cookies and social trackers blocked.

Developer: Microsoft.

Supported operating systems: Android, iOS, Linux, MacOS and Windows.

License: proprietary software.

Although Chrome is the most popular it is not without its flaws:

1) It is the most criticized browser for its high memory usage vs other browsers.
2) They are not completely transparent with their data privacy policy – the data they collect from us and what they do with it.

Some of the known items that google tracks:

- Google searches
- Google Maps usage
- YouTube viewing history
- Device configuration
- Location data
- Cookies for marketers to use for advertising purposes

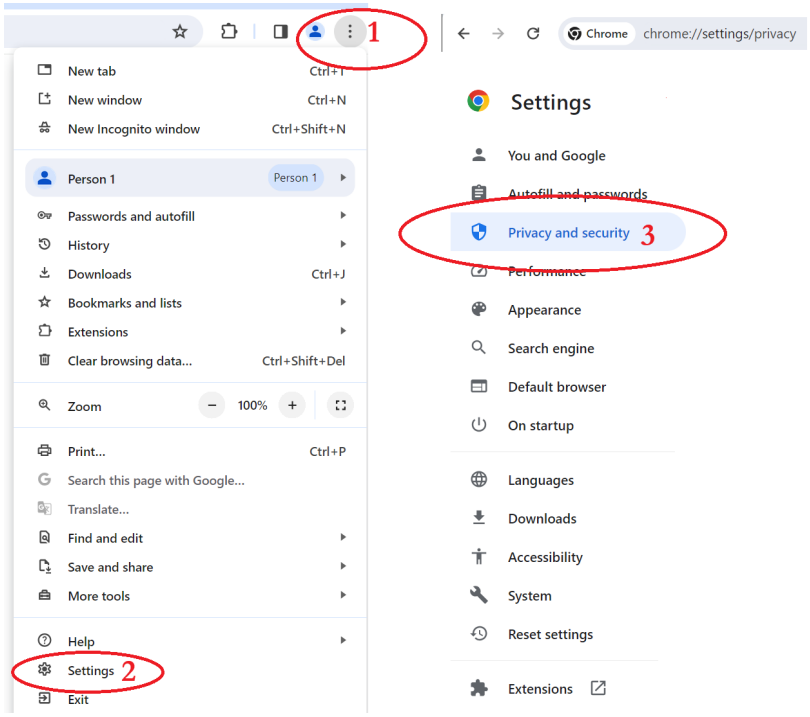
- ...and more unknown items

Let's review a few privacy items for Chrome, Safari and Edge and learn to clear up some of our data:

Google Chrome

1) Open Chrome, click on the **three dots** in the top right corner.
2) Click Settings
3) Click Privacy and Security

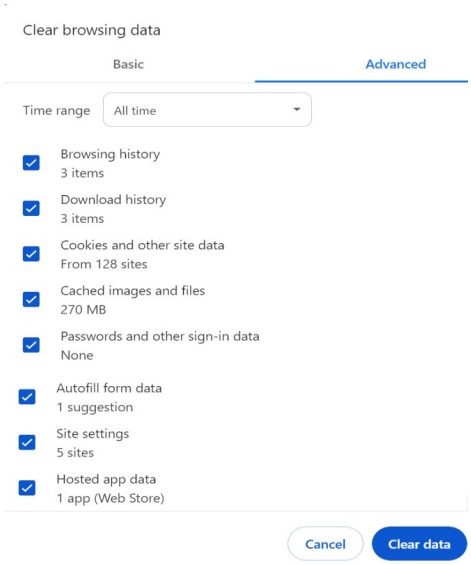
To make quick changes to your privacy settings you can enter **chrome://settings/privacy** in the URL at any time.



Items that we recommend reviewing are:

Clear browsing data → Advanced:

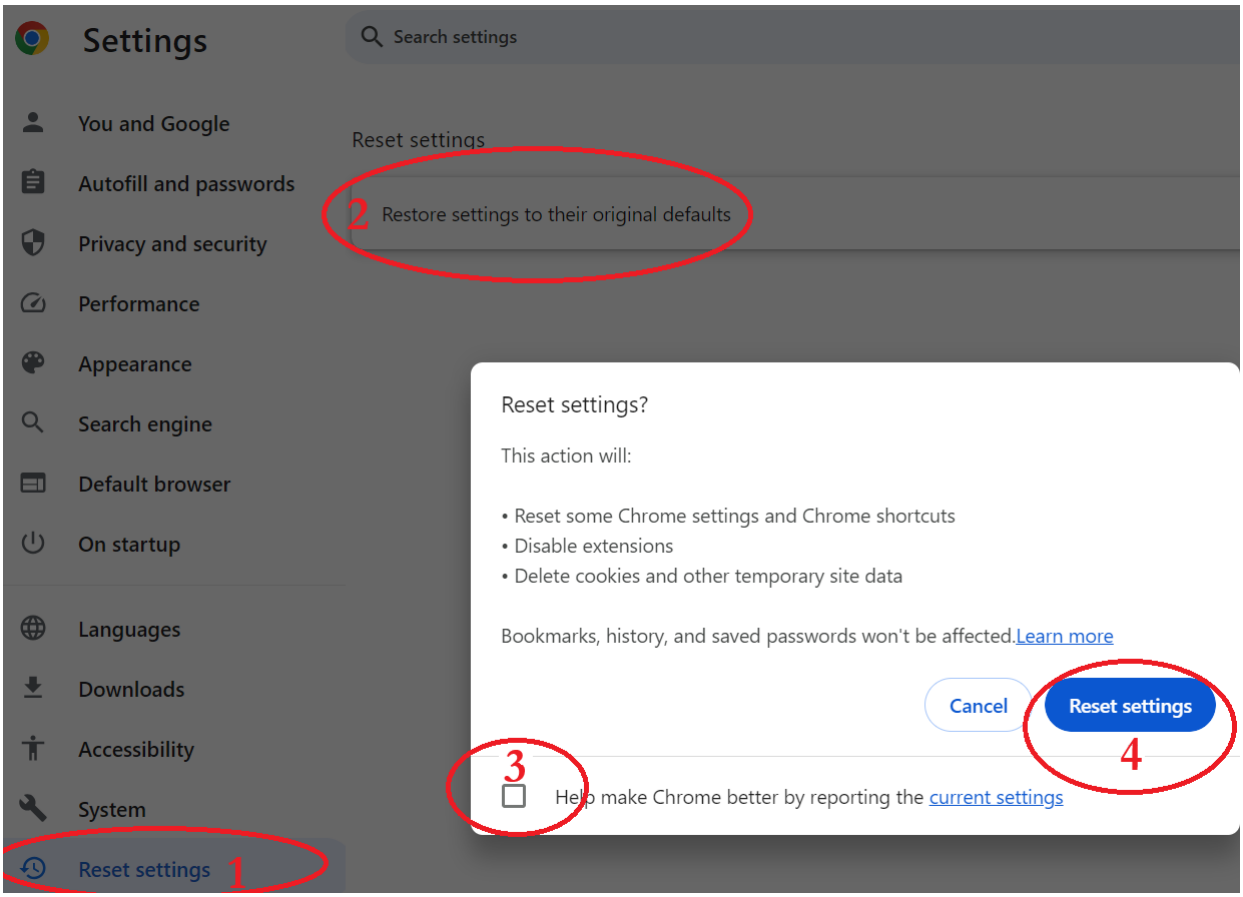
Browsing history, Download history, Cookies and other site data, cached images and files, Passwords and other sign-in data, Autofill form data, Site settings and Hosted app data.



NOTE ****Selecting these settings will remove the data from your browser every time it is closed****

Other settings should also be reviewed. If after making any changes you need to revert due to an unexpected behavior, settings can be reset back to their defaults by doing the following:

1) Click on Reset Settings
2) Restore settings to their original defaults
3) Uncheck the box which will report current settings
4) Click the Reset settings button

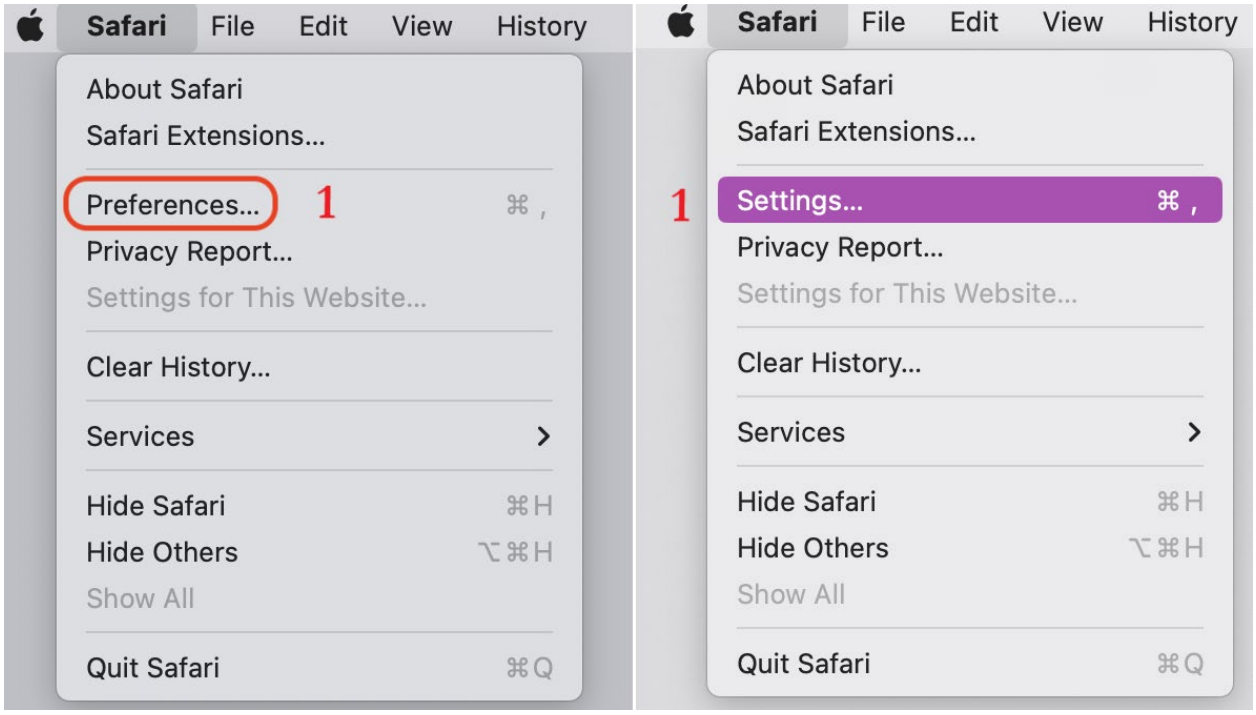


Mac Safari

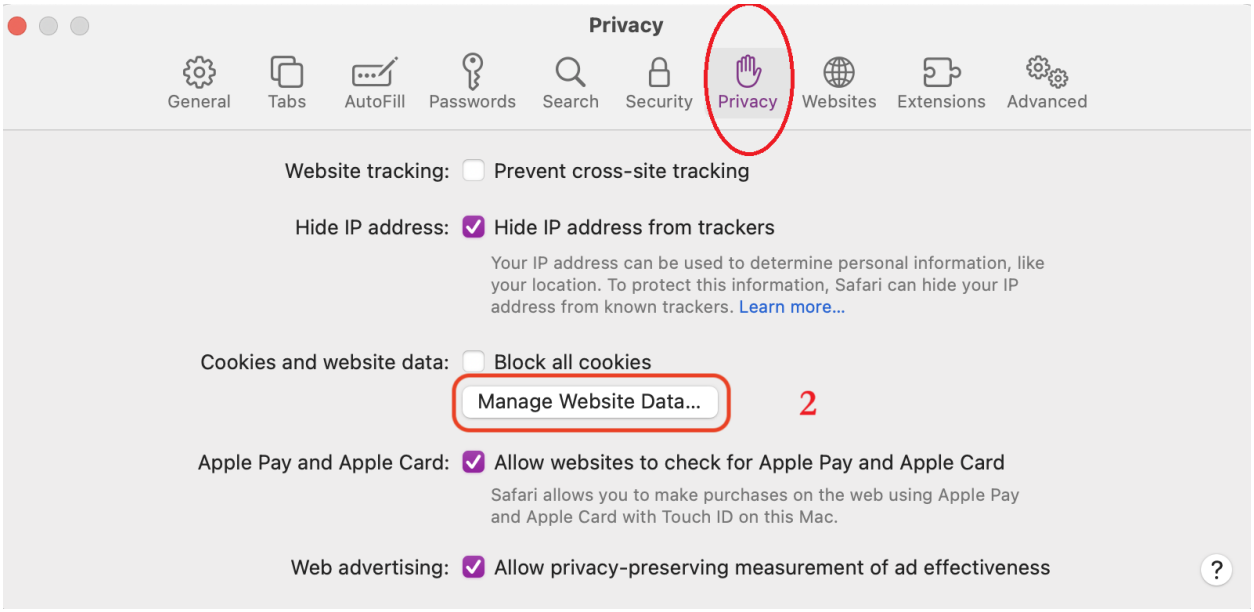
After much research on Safari versions 17.1-11, I have not been able to find an automated way to clear the web browser history, cookies, etc., automatically on close. Although you can prevent cookies from ever being created in the first place, this may stop some websites from functioning properly. Instead, we only have a one time option to clear the data. First, I will walk you through clearing up the browser history and then I will walk you through clearing caches.

In the Safari menu:

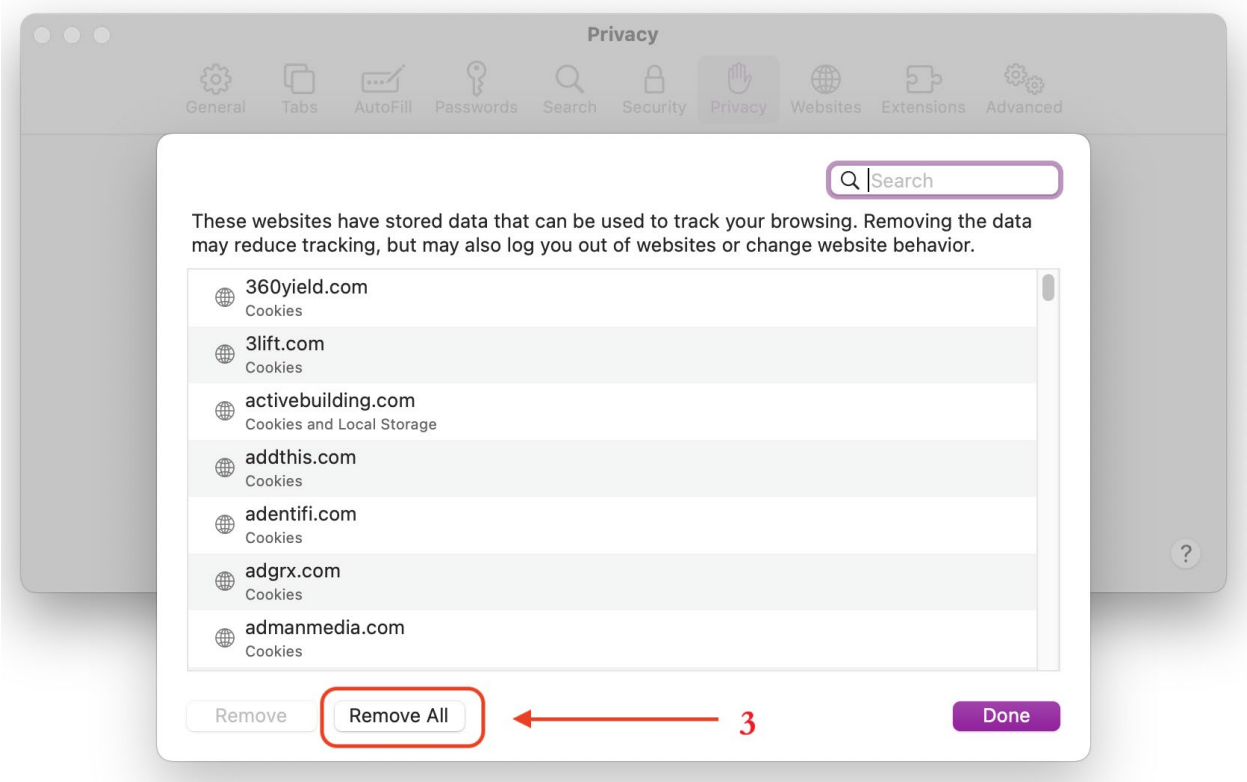
1) Choose "Preferences..." (macOS Monterey and older) or "Settings" (macOS Ventura)



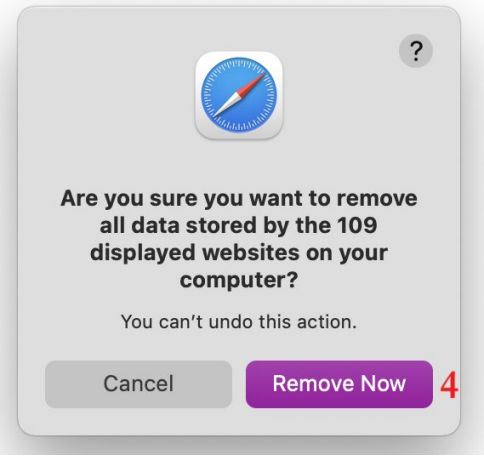
2) Click on 'Privacy' at the top of the new window then click the 'Manage Website Data' button



3)Click “Remove All”



4) Click “Remove Now”



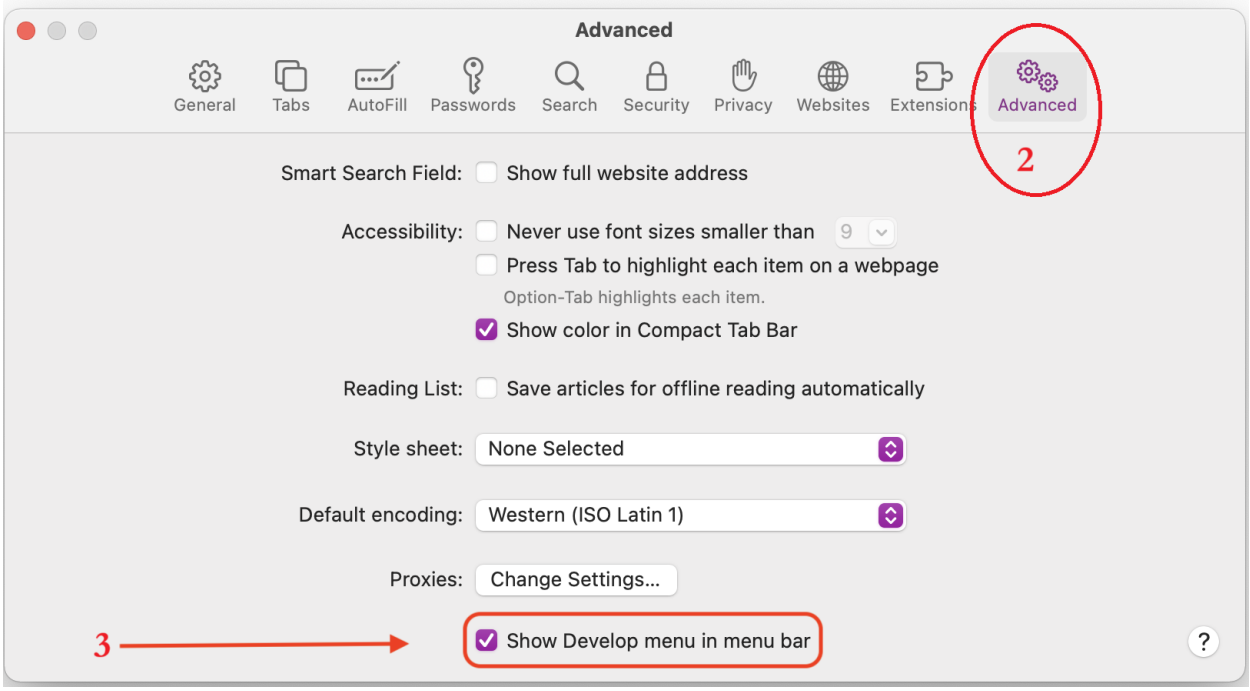
To clear caches:

1) In Safari, click on Preferences or settings as before

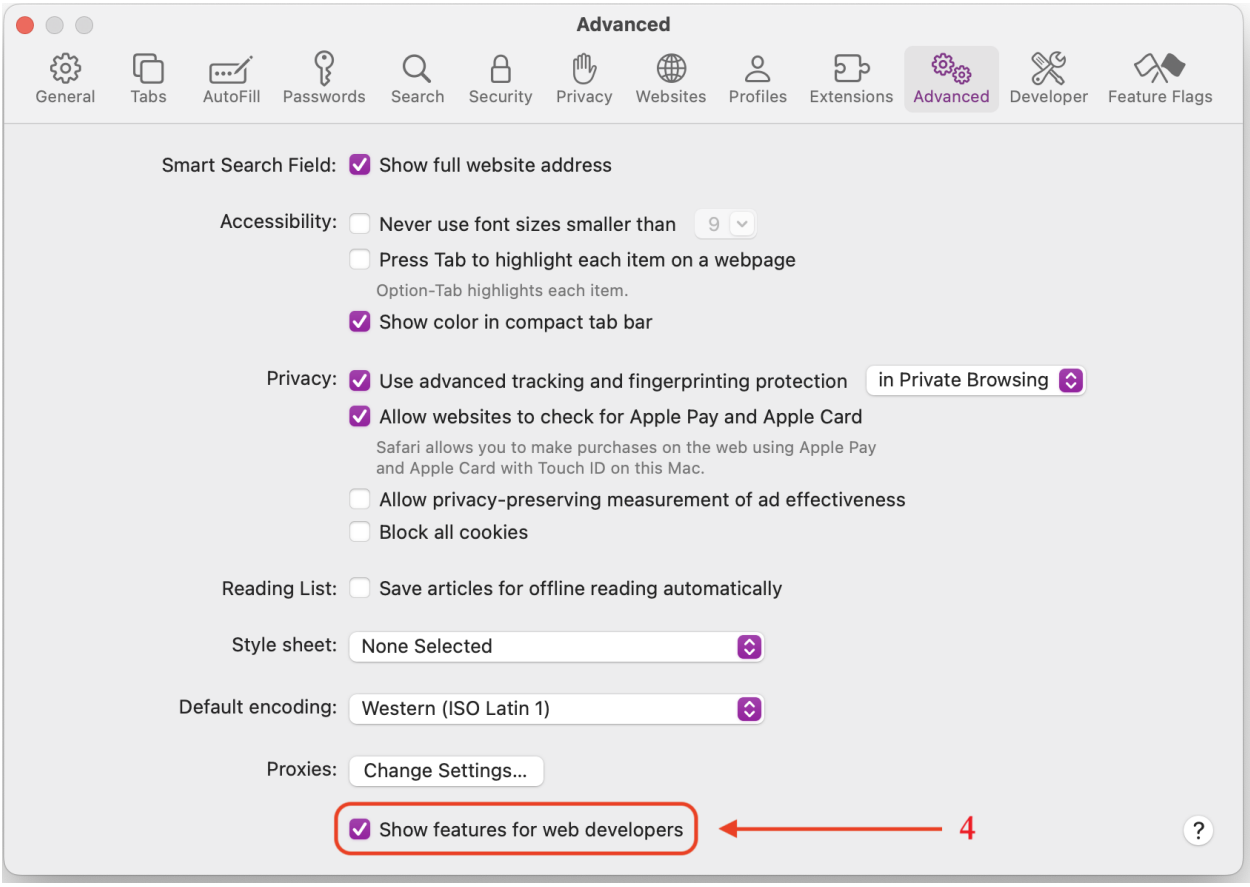
2) Click on Advanced

3) Enable the checkbox to 'Show Develop menu in menu bar' or 'Show features for web developers,'

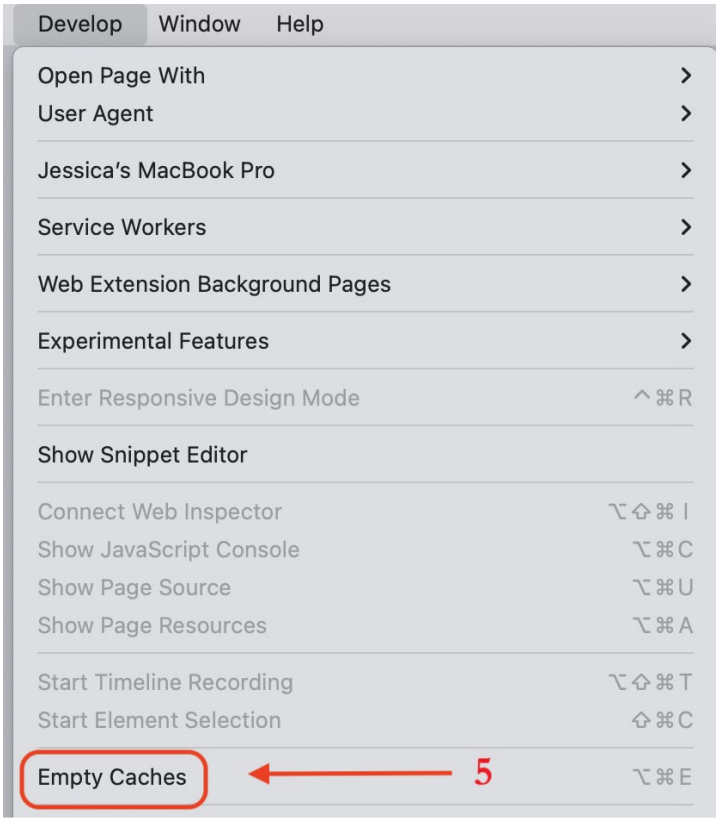
depending on which version of Safari you have.



4) Next, you'll want to clear caches. To do so, you need to enable 'Develop' mode to clear Safari caches:



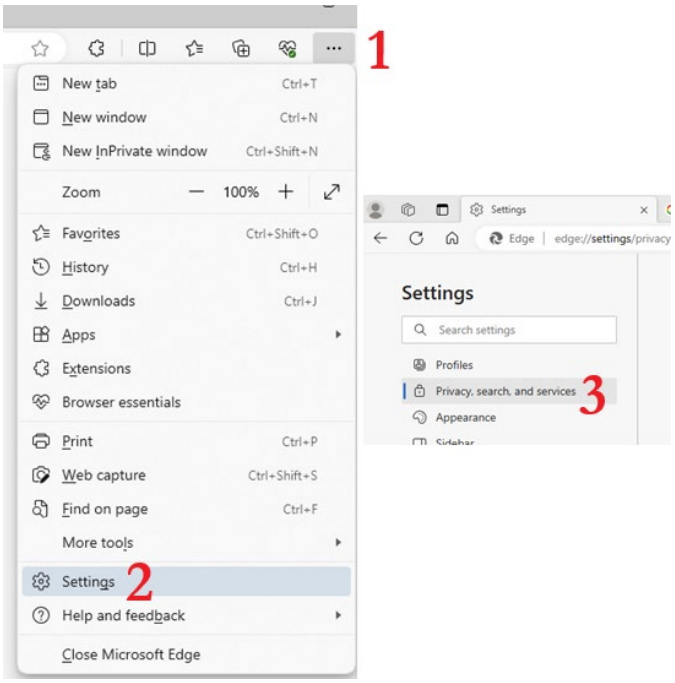
5) Lastly Click on Develop and Empty Caches



Microsoft Edge

To get to your privacy settings do the following:

1) Open Microsoft Edge, click on the **three dots** in the top right corner
2) Click on **Settings**
3) On the left-hand column click on **Privacy, search and services**



To make quick changes to your privacy settings you can enter **edge://settings/privacy** in the URL at any time.

Items that we recommend reviewing are:

Clear browsing data on close: Browsing history, Download history, Cookies and other site data, cached images and files, passwords, Autofill form data (including forms and cards) and Site permissions.

Privacy: Send "Do Not Track" requests. (Enable this setting)

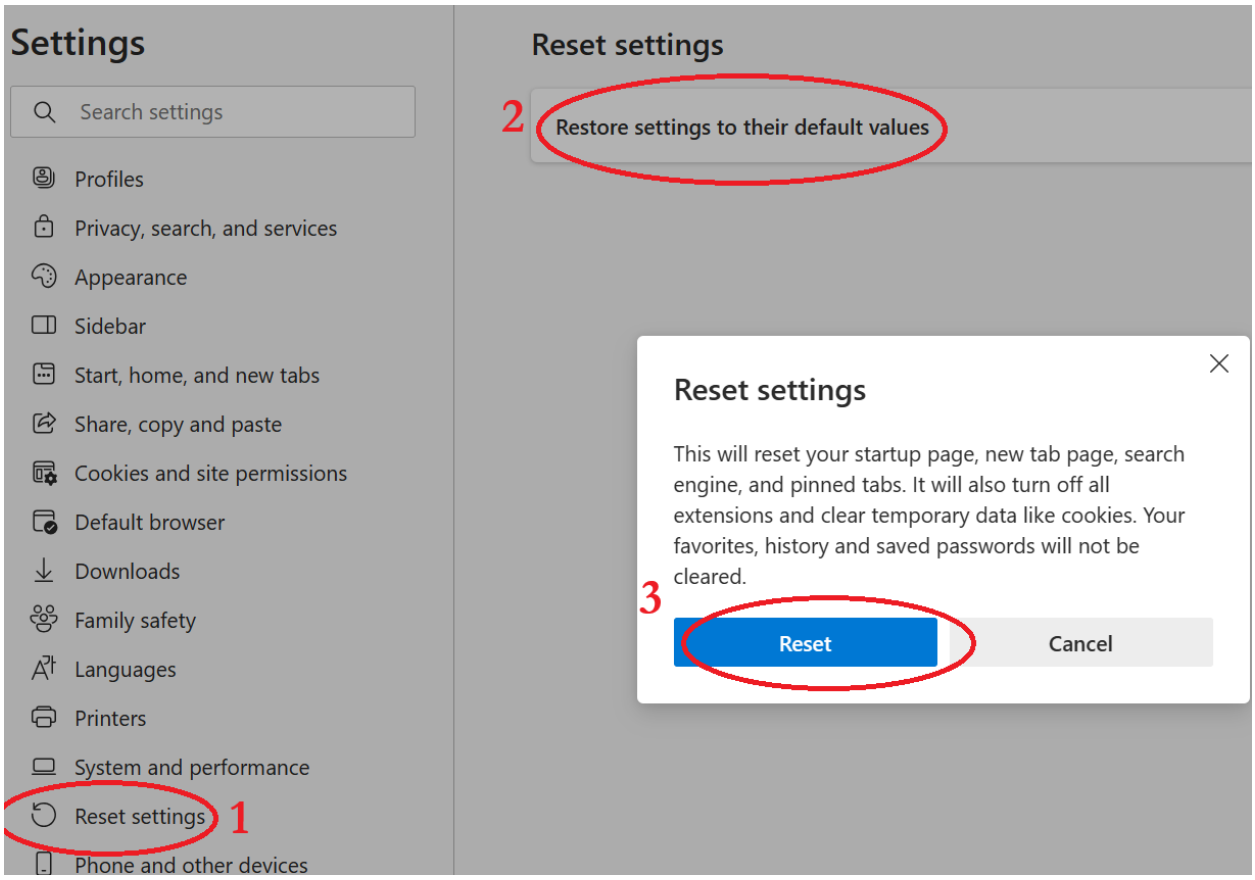
Allow sites to check if you have payment methods saved.

NOTE ****Selecting these settings will remove the data from your browser every time it is closed****

Other settings should also be reviewed. If after making any changes you need to revert due to an unexpected behavior, you can reset your settings back to the default by doing the following:

As shown above, open Microsoft Edge, click on the **three dots** in the top right corner and go to **Settings**

1) Click on Reset Settings
2) Restore settings to their default values
3) Click the Reset button prompt



As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at security@bsd.uchicago.edu .