INTERNET BROWSER PRIVACY TIPS IN BROWSER SETTINGS

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of March 2025.

This handout discusses various options that can enhance a user's privacy in four of the most popular internet browsers: Google Chrome, Safari, Microsoft Edge and Samsung Internet.

Internet browsers are the first step to accessing the internet, while a search engine allows you to search the internet once you have gained access. Both internet browsers and search engines can be used to increase your online privacy and help control your personal information. Popular browser and search engine products such as those mentioned above provide in-browser privacy settings for users.

For survivors of abuse and stalking, using these options may increase their privacy and safety, particularly if they are concerned that an abusive person is monitoring their activity. They can also help survivors have more control over how their personal information is collected and stored when they are online. However, browser privacy options are not going to protect from remote spying or monitoring if an abusive person is either using remote management tools or has downloaded malicious software, such as stalkerware onto a targeted device. To learn more about stalkerware and other online privacy tips, visit www.techsafety.org.au/resources-women.

A few options that can enhance a user's privacy when browsing the internet include the following:

Private browsing allows users to surf the internet without the browser collecting search history, the pages you visit or your AutoFill information. This is helpful if a survivor is concerned that someone may be monitoring their internet activity by going through the browser history. However, private browsing will not prevent someone from knowing what you're doing online if they are looking over your shoulder or are monitoring your device with remote access tools.

Do Not Track is a setting that sends a signal to websites, analytics companies, ad networks, and plug-in providers, amongst others, to stop tracking your activity. Whether they honour the signal request, however, is another story – it is voluntary to do so and not enforced, therefore we recommend reviewing their privacy policies to

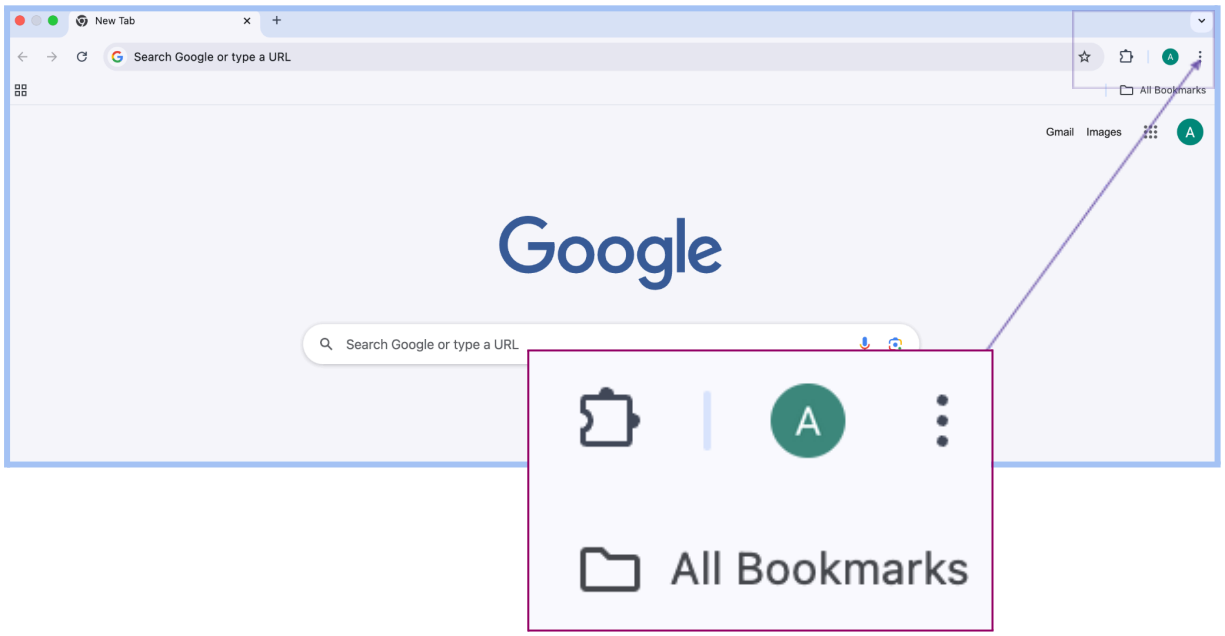
check this. This feature is only for third-party tracking, which often tracks users for behavioural advertising purposes; it doesn't prevent the website that you're visiting from collecting information about you.

All the browsers discussed in this handout allow users to delete their browser history. Regularly deleting your browsing history can increase privacy, however if someone is monitoring your online activity, deleting your browser history may appear suspicious.

Virtual Private Networks (VPN)

Privacy-aware users may use a Virtual Private Network (VPN) technology to mask their online activities. A VPN creates an encrypted tunnel for your data, this includes protecting your online identity by hiding the IP address and strengthens your safety when using public Wi-Fi or unsecure networks. Using a VPN can also help prevent data and bandwidth throttling, access geo-blocked services and ensure secure downloading and uploading of files from the internet. VPN software can be installed on devices as well as internet browsers and routers. It is best to do due diligence on the best service to engage with by searching online.

Google Chrome



Private Browsing (Incognito Mode)

- In a new window, click on the **three dots** (customisation and control menu, shown above).
- Select **New Incognito Window**.
- A new window will open with a message explaining incognito mode. You will remain in incognito mode until you close this browser window.

Do Not Track

- Select the **three dots** on any Chrome window and select **Settings**.
- Once settings are open > select **Privacy and Security** > **Third Party Cookies** > ensure **Block third-party cookies in Incognito** is switched on.
- Additionally, you can turn on **Do not track requests with your browsing traffic**. Any effects of this tool will depend on the website responding to the request.

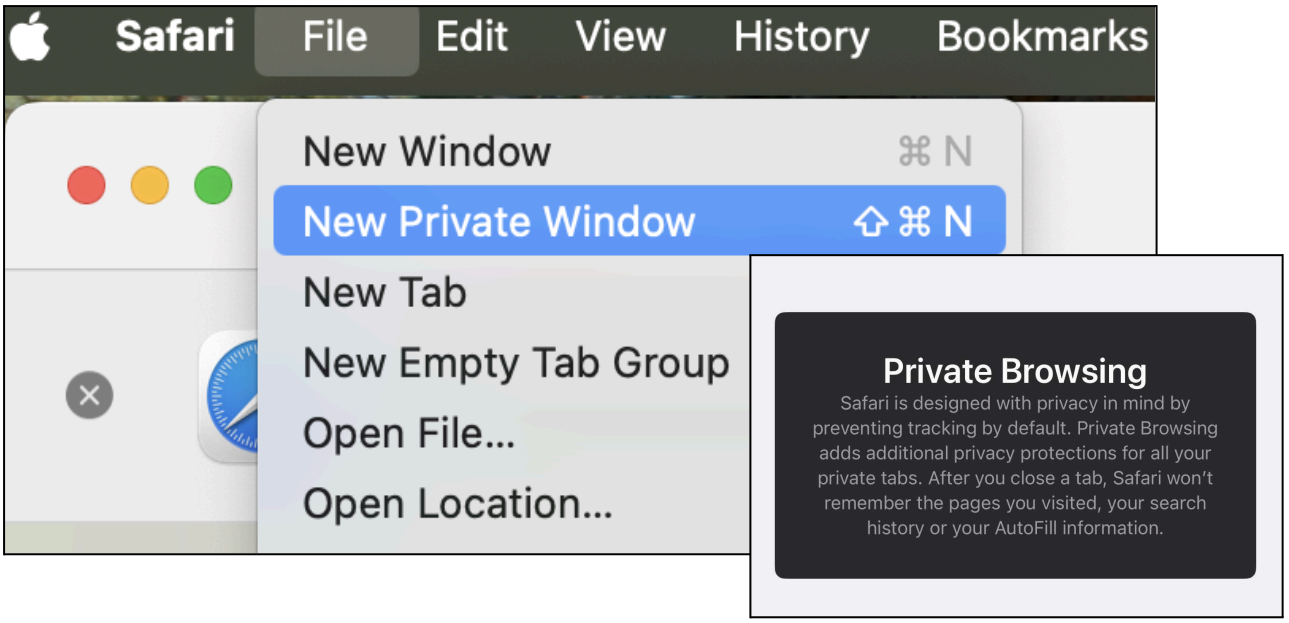
History

- Select the **three dots** and select **History**.
- Select **Delete Browsing Data**. You can select to view **Basic** or **Advanced** browsing data, or you can choose certain pages and select which items you'd like to remove. Deleting selected web pages might be a good option if you are worried deleting the entire history might appear suspicious.

Additional Privacy Options

- Click on the **three dots** and select **Privacy and Security**, under security you can explore **Safe Browsing** options, either enhanced protection, standard protection or no protection.
- Under the same security page, you can also explore advanced settings to further enhance and secure your internet browsing experience.
- Google now also offers **Privacy and Security Checkup** tools that allows you to review your preferences and settings of any Google products you use. These tools are available under the **Privacy and Security** page or by searching 'Google safety and privacy check' on your web browser.

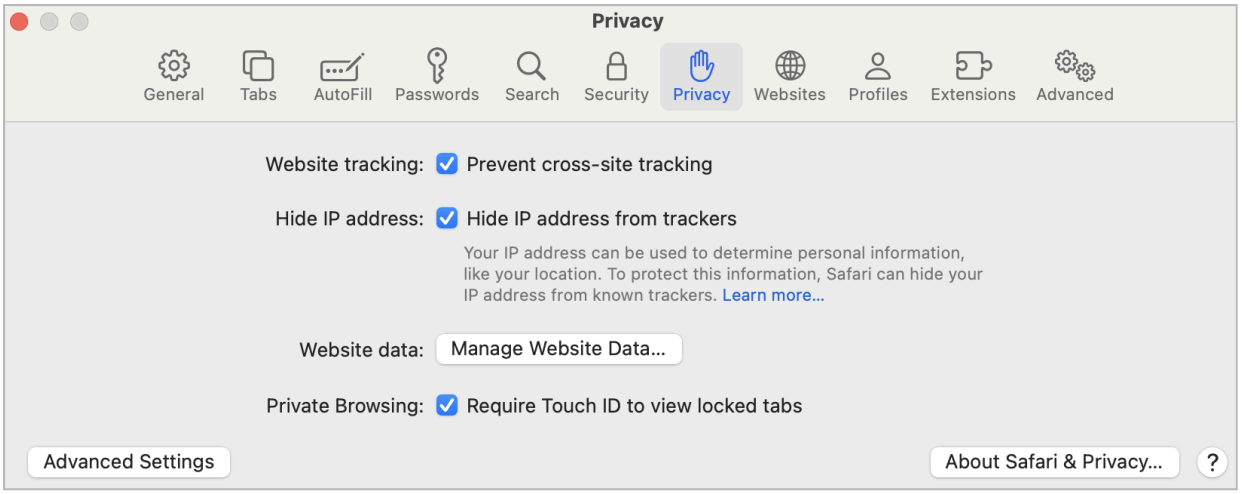
Safari



Private Browsing

- Apple's Safari was the first to introduce private browsing.
- Click **File** and choose **New Private Window** (see image above).
- On Apple Iphone and Ipads, open **Safari** and slide over to **Private**, open a new tab with the **+** button
  .
- When in Private Browsing mode, your address and search field will have a dark background with white text.
- To stop using Private Browsing, close the Private Browsing window or switch to another Safari window that isn't using Private Browsing.

Do Not Track



- Once **Safari** is open, open **Settings** and select the **Privacy** tab (as seen in image above).
- On this page you can explore Website Tracking, Hide IP address, Manage Website Data and Private Browsing.

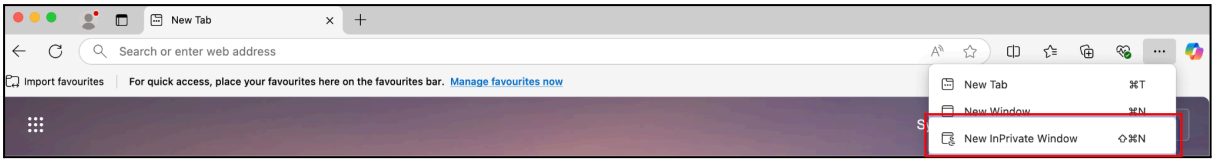
History

- Go to **History**, and select **Clear History**.
- Select from the **drop-down menu** the period you would like your history data to be deleted.
- Click **Clear History**.

Additional Privacy

Go to **Settings** and select the **Advanced tab**. Here you can block cookies and enable privacy preserving measurements.

Microsoft Edge



InPrivate Browsing

- In a new window, click on the **three dots** in the top right corner click **New InPrivate window**.
- A new window will open with an explanation of **InPrivate Browsing**. You will remain in this mode until you close this browser window.
- To ensure you're browsing privately in Edge, look for the blue logo located in the top left corner of the window.

Do Not Track

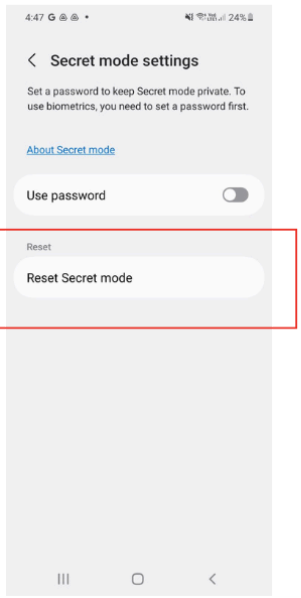
- In a new window, click on the **three buttons** at the top right corner then select **Settings**.
- Select **Privacy, Search and Service** from the left-hand side menu, in this section you can select your preferred **Tracking Prevention**, either **Basic**, **Balanced** or **Strict**.

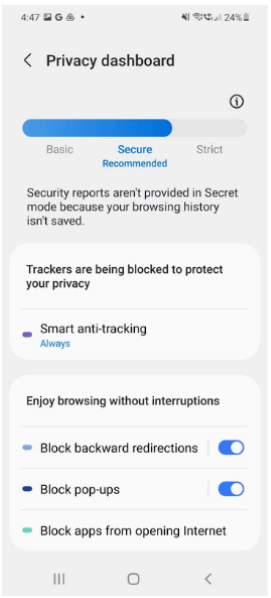
Additional Privacy Options

Through **Settings**, you can review the following additional privacy options.

- Under **Privacy, Search and Service** you can **Delete Browsing Data** and adjust Privacy to **Send "Do Not Track" Requests**.
- Under **Security**, you can also **Enhance Your Security on The Web** to either **Balanced** or **Strict**.
- Select **Cookies and Site Permissions** from the left hand side menu to **Manage and Delete Cookies and Site Data** as well as managing **Site Permissions** such as location, camera and microphone.

Samsung Internet





Private Browsing

After opening the Samsung Internet application, open a **new tab** and select **Turn on Secret Mode** in the bottom left hand corner. Any cookies or browning history for any website visited will be erased from the phone as soon as all Secret Mode tabs are closed.

Do Not Track

After opening the **Samsung Internet application**, tap the **Menu** (three horizontal lines on the bottom right corner) and select **Privacy**. On this page you can explore and turn on the **Smart Anti Tracking** feature, this will block cookies and trackers that follow on each website you may interact with.

History

To delete History, open **Samsung Internet**, tap the **Menu** and select **Settings**. From here, open **Personal Browsing Data** and select **Delete Browsing Data**, choose your desired option and proceed to **Delete Data**.

Additional Privacy Options

In the same **Privacy** page outlined above, you can also turn on notifications to be **Warned About Malicious Sites**, **Block Automatic Downloads** and **Switch to Secure Connection**.

- Under the **Privacy** page, select **Personal Browsing Data** and open **Secret Mode Settings**, in this section you can set a password to keep Secret Mode private.

- Under the **Settings** Menu, navigate to the **Permissions page**. Here you can adjust permissions for Location, Camera, Microphone, Files and Media and Phone.

Alternative safety tools and resources

Alternatives

There are alternative private browsers outside of the built in functions mentioned above, many of these are free or have monthly fees associated. Examples to explore include Brave, Tor, Iridium, DuckDuckGo, Epic Privacy Browser and LibreWolf. Cybersafety and privacy tools offered by these browsers may include the following: private browsing, encrypted connections, blocking of trackers, cryptominers and fingerprinters, controlling of activity logs, password monitoring, email protection, and deletion of cookies.

Think About Your Safety

Survivors are often guided to turn off their technology, delete accounts or stop using technological devices completely if they want the abuse to stop. This guidance will not always protect survivors and may further isolate them from their support network, potentially placing them in further danger. When working with survivors, it is critical to integrate technology safety planning into holistic safety planning. For example, some survivors choose to use their computer privacy and security settings to ensure their browser always opens in private browsing mode and erases their history on exiting. Others might opt to continue using their usual browser for general online activity, while using a private browser for their confidential online activities. When compiling your Safety Plan, think about your safety first by considering what may happen if you hide or remove all evidence of your online activity.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.