INTERNET BROWSER PRIVACY TIPS IN BROWSER SETTINGS #KNOWTECHABUSE

Please note that the contents of this document should not be regarded as legal advice. The information contained within is current as at November 2022.

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

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 physically monitoring their device 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 stalkerware/spyware software 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 stalkerware/spyware or 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.

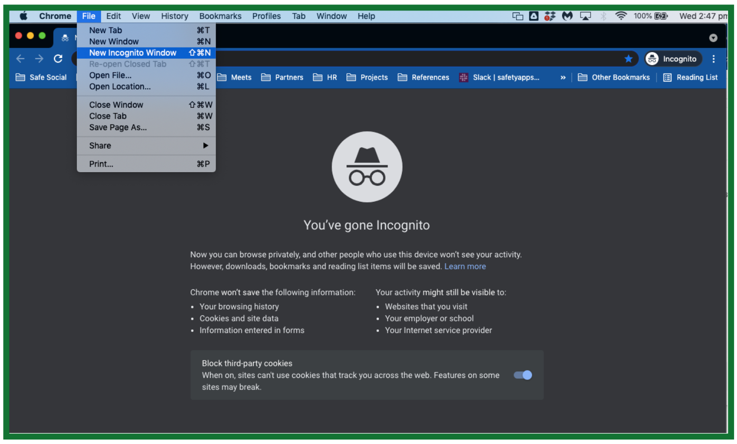
Virtual Private Networks (VPN)

Privacy-aware users may use a Virtual Private Network (VPN) technology to mask their online activities. A VPN encrypts your internet traffic on unsecured networks to protect your online identity, hide your IP address, and shield your online data from third parties. Using a VPN can also help with avoiding targeted bandwidth throttling, accessing your home, education or work networks remotely, saving money on flights, hotels and car rentals, improving security when using public Wi-Fi, protecting your mobile devices, ensuring secure downloading and uploading of files, avoiding online shopping discrimination, and protecting your right to privacy. VPN software can be installed on iOS, android and Linux operating systems, desktop computers, laptops, smartphones, internet browsers and routers.

Google Chrome

Private Browsing (Incognito Mode):

- In a new window, click on the Chrome menu icon.
- Choose "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.



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites that you visit
- Your employer or school
- Your Internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Do Not Track:

- Slide the 'Block third-party cookies' toggle to ON in the main screen.
- Alternatively, click on the Menu icon in the top right corner and head to "Settings" → "Advanced" → "Privacy and Security" → "Cookies and other site data" and ensure "Block third-party cookies in Incognito" is selected.
- Additionally, Google uses "Protect My Choices," which instals opt-out, site-specific cookies on your computer. This requires installation of an extension instead of just a change in settings and it cannot be added in Incognito or in

guest windows. It also doesn't stop websites from collecting information about your activity, it just stops them from showing you targeted ads.

  - Visit the Chrome web store and install "Protect My Choices."
  - A pop-up will confirm that it has been added to Chrome.

History:

- Click on the Menu icon in the top right corner and choose "History"
- Then "Show full history" and "Clear browsing data". You can select a "Time range" or select "All time" to delete the entire "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:

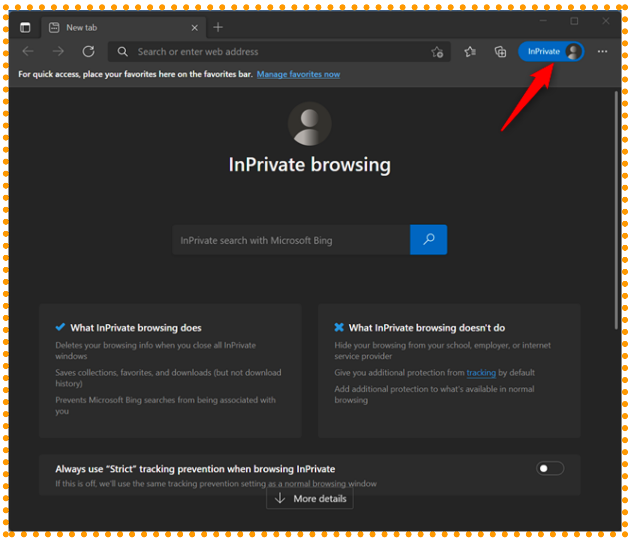
- Click on the Menu icon in the top right corner and choose "Settings" or navigate to the "Settings" section from the History page.
- Here you can determine whether Chrome can (1) enable phishing and malware protection, (2) use a prediction service to help complete searches and URLs typed, (3) offer to save your passwords, and (4) use Autofill for webforms.
- Visit the "Safe Browsing" section within "Security" to manage protections around dangerous websites, downloads, and extensions, and to warn you about password breaches.
- Google now also offers Privacy Checkup that allows you to review your privacy settings of any Google products you use, such as YouTube. Visit https://myaccount.google.com/privacycheckup/ for more information.

Microsoft Edge

First off, it's important to know that Microsoft has replaced Explorer with Edge (for Windows 10 users). The last version of IE, Internet Explorer 11 ended support for Windows 10 Semi-Annual Channel on 15 July 2022. We recommend updating to a new browser if you are still using IE.

InPrivate Browsing:

- In a new window, click on the "Settings and more" button at the top right corner then click or tap on "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 right-hand corner of the window.


New tab
Search or enter web address
InPrivate
InPrivate search with Microsoft Bing
More details

For quick access, place your favorites here on the favorites bar. Manage favorites now

InPrivate browsing

✓ What InPrivate browsing does

Deletes your browsing info when you close all InPrivate windows

Saves collections, favorites, and downloads (but not download history)

Prevents Microsoft Bing searches from being associated with you

✖ What InPrivate browsing doesn't do

Hide your browsing from your school, employer, or internet service provider

Give you additional protection from tracking by default

Add additional protection to what's available in normal browsing

Always use "Strict" tracking prevention when browsing InPrivate

If this is off, we'll use the same tracking prevention setting as a normal browsing window

Do Not Track:

- In a new window, click on the "Settings and more" button at the top right corner then select "Settings".
- Select "Privacy and Services" from the left-hand side menu and scroll down to toggle ON the "Tracking prevention" request.

Additional Privacy Options:

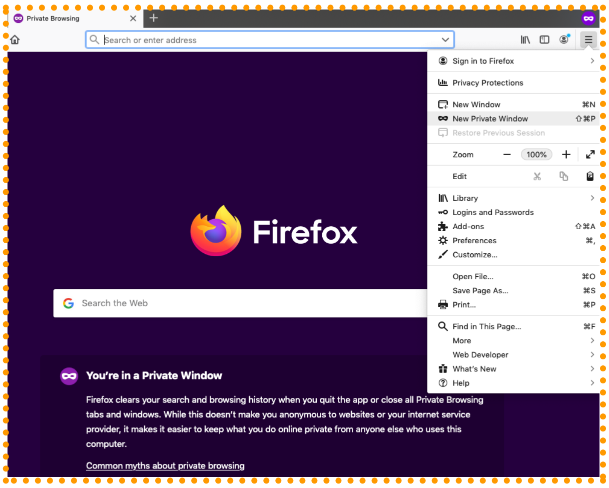
Click on the "Settings and more" button at the top right corner then select "Settings".

- Under "Privacy, search and services" you can change your level of tracking prevention, clear your browser history deleted on exit or you can delete your current history.
- You can choose one of the three options – "Basic", "Balanced" or "Strict".
- If you want InPrivate to always default to the harshest anti-tracking, toggle ON "Always use "Strict" tracking prevention when browsing InPrivate".
- Edge version 88 and higher offers a password monitor to alert you if one of your passwords may have been compromised and a password generator to suggest strong passwords for new accounts. To use both features, go to "Settings > Profiles > Sync", then click the "Turn on Sync button".
- To use the password monitor for data breaches, enable the switch for "Show alerts when passwords are found in an online leak".
- To use the password generator, head to "Settings > Profiles" and turn on the switch for "Offer to save passwords". The switch for "Suggest strong passwords" should then turn on as well. The next time you create a new account for a website, click in the password field and Edge should suggest a strong and secure password. Click "Refresh" to choose and select a password.

Mozilla Firefox

Private Browsing:

- In a new window, click the menu icon in the top right corner and choose "New Private Window."
- A new window will appear with the tell-tale purple "mask" icon in the top right-hand corner explaining Firefox's Private Browsing option. You will remain in this mode until you close this browser window.



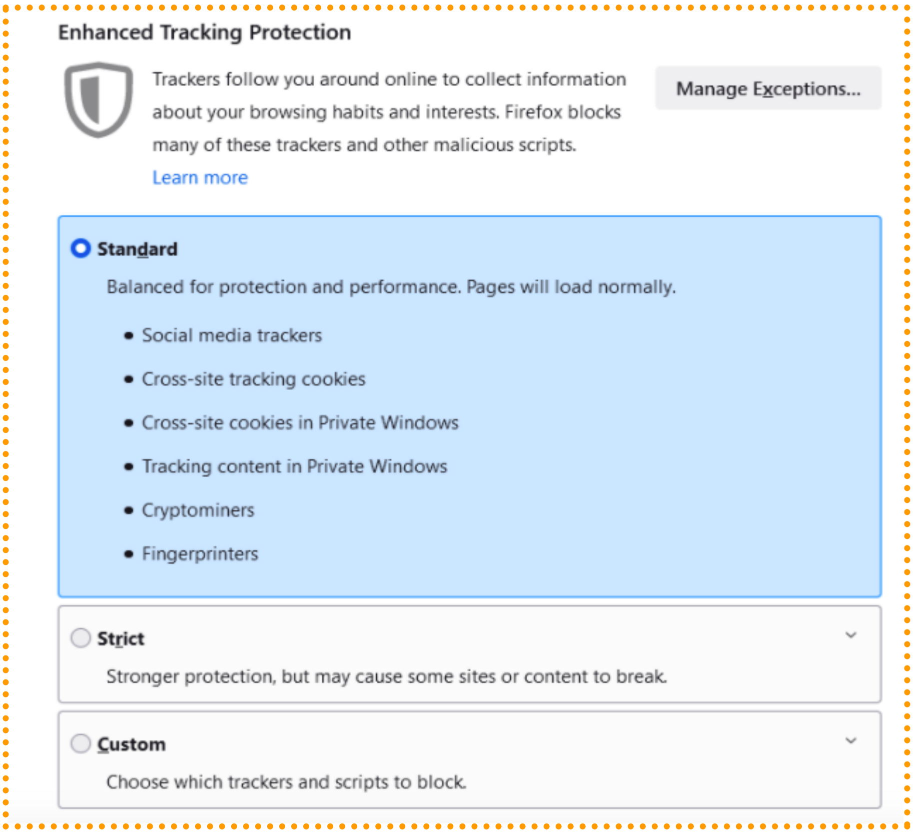
You're in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

Do Not Track:

- The "Tracking content" remains on by default in private windows.
- Because "Enhanced Tracking Protection" under "Browser Privacy" is enabled by default within Firefox, it doesn't matter whether the "Standard", "Strict" or "Custom" setting is selected as everything that can be blocked will be blocked.
- Under "Enhanced Tracking Protection," choose "Always" under "Do Not Track".



Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

● Standard

Balanced for protection and performance. Pages will load normally.

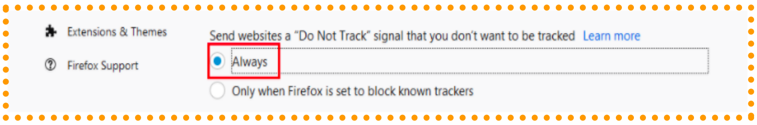
- Social media trackers
- Cross-site tracking cookies
- Cross-site cookies in Private Windows
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

○ Strict

Stronger protection, but may cause some sites or content to break.

○ Custom

Choose which trackers and scripts to block.



Send websites a "Do Not Track" signal that you don't want to be tracked Learn more

● Always

○ Only when Firefox is set to block known trackers

History:

- Under "Privacy & Security" and "History", you can choose Firefox to "Never remember history". Here you can also "Use custom settings for history" to select the "Always use Private Browsing mode" setting. N.B. you will need to restart Firefox to enable these features.
- You can also "Clear Recent History" in this window.

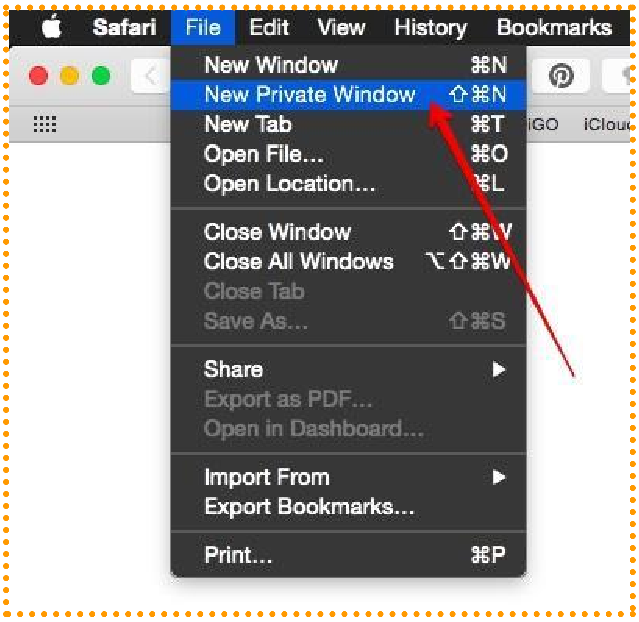
Additional Privacy Options:

- Cross-site tracking cookies are now disabled by default for all Firefox users.
- Mozilla is incorporating the Global Privacy Control (GPC) as a pre-release feature available for experimental use in Firefox Nightly. The GPC -- required under the California Consumer Protection Act (CCPA) and Europe's Global Data Protection Regulation (GDPR) -- tells websites not to sell or share your personal data.
- Under "Enhanced Tracking Protection" or by clicking the "shield" to the left of the address bar you can see what trackers Firefox has blocked.
- Passwords can be managed via "Firefox Lockwise".
- You can also check to see if you've been part of a known data breach via "Firefox Monitor".

Safari

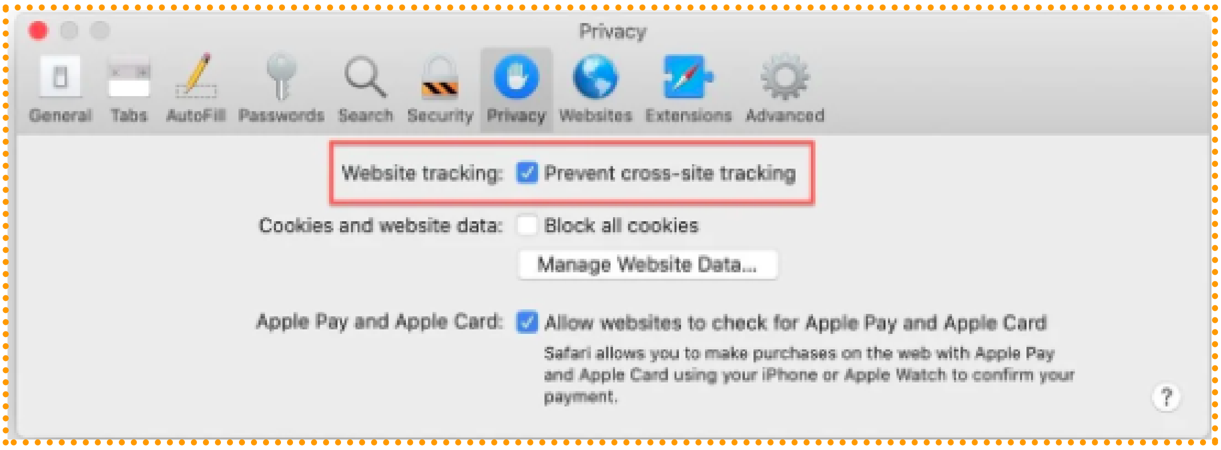
Private Browsing:

- Apple's Safari was the first to introduce private browsing.
- Click File and choose "New Private Window."
- 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:

- Go to Preferences, and select the Privacy Tab.
- Select "Website tracking: Prevent cross-site tracking".



Website tracking: ☑ Prevent cross-site tracking

Cookies and website data: □ Block all cookies

Manage Website Data...

Apple Pay and Apple Card: ☑ Allow websites to check for Apple Pay and Apple Card

Safari allows you to make purchases on the web with Apple Pay and Apple Card using your iPhone or Apple Watch to confirm your payment.

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 Preferences, and select the Privacy Tab.
- You can limit or block websites cookies and website data. You can also "Remove All" website data".
- You can also limit a website's use of your location to provide services and features. You can choose to be prompted before a website uses your location or deny it without prompting you first.

Alternatives

Lesser-known privacy-oriented alternatives include Brave, Tor, Iridium, DuckDuckGo, Ungoogled Chromium, LibreWolf, GNU Icecat, Waterfox, Bromite (Android) and Pale Moon. 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

Victims often want to stop the abusive behaviour by getting rid of the technology or their digital trail. However, for some abusive individuals, this may escalate their controlling and dangerous behaviour as it can make them feel as though their control is threatened. 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.