2025.12.09.1

RESIST KIT

INFO

WEB BROWSERS & ONLINE PRIVACY

Modern browsers collect enormous amounts of data about how you search, shop, bank, and move around the internet. Much of this is baked into their design because your behaviour is extremely valuable.

Australia's new Age Verification requirements start 27 December 2025, meaning search engines such as Google Chrome, Microsoft Edge/Bing and Apple/Safari will become even more tightly connected to identity-based systems, meaning your browsing environment becomes a key point where identity checks can be pushed or nudged.

This guide helps you reduce that creep as much as possible.

RECOMMENDED PRIVACY-RESPECTING BROWSERS

The following browsers are widely used in privacy and security-conscious communities. They avoid the identity-linking features built into Chrome, Edge, and Safari.

Desktop:

- LibreWolf - hardened Firefox with strict privacy defaults, no telemetry, and built-in tracking protection
- Mullvad Browser - created with Tor Project; designed to minimise browser "fingerprinting." Excellent for research and general browsing.

Mobile / Android:

- Vanadium (GrapheneOS) - strongest browser option on Android, with strict sandboxing and mitigations.
- Firefox + Containers - a good, user-friendly option if switching fully feels too big a step.

BROWSER HARDENING CHECKLIST

These steps reduce how much data is created, stored, or linked back to you.

1. Don't Sign Into the Browser

Most privacy loss happens the moment you sign in:

- It links your entire browsing history to your account.
- It synchronises data across devices.
- It creates a near-perfect profile of your behaviour.

You can browse the web perfectly well without signing in.

Get more resources & kit here: **www.MyResistKit.com**

ALIGNED COUNCIL OF AUSTRALIA

RCR .media

WEB BROWSERS & ONLINE PRIVACY *Continued*

INFO

2. Turn Off Sync (History, Bookmarks, Passwords)

Syncing sends your information to big tech servers by default. Reduce this by turning off:

- Search and browsing history
- Auto-fill
- Password sync
- Payment methods (e.g. saved credit card details)

If you need help remembering your passwords, use a dedicated password manager (e.g. Proton Pass) - instead of web browsers (like Google's) built-in one.

3. Install a Content Blocker

A content or tracker blocker stops websites from collecting your data (such as your browsing habits, device info). It does this by blocking scripts and cookies at the application/browser level. Content Blocker is different to a VPN, which masks your traffic and hides your IP address at the network level (for more information on VPN's check out our VPN guide in the www.MyResistKit.com).

Content blockers recommended:

- uBlock Origin (free, highly effective)
- Add lists for anti-tracking and anti-fingerprinting where available.

This reduces ads, cuts down on behavioural profiling, and speeds up your browsing.

Note, some privacy-focused browsers such as those recommended above may already have a content blocker built in to them.

4. Use Separate Browser Profiles for Different Tasks

Splitting your activities stops companies from linking your behaviour across different parts of your life. Create separate profiles or use separate browsers for:

- Banking only
- Government portals only
- Social media only
- Shopping / general browsing
- Work use

This is one of the most powerful privacy steps you can take.

E.g. Your bank does not need to know you were researching homeschooling or looking at medical information ten minutes earlier.

5. Clear Cookies Regularly

Cookies are tiny files your browser drops while you browse. Many companies collect them to build detailed insights about you.

Good practices:

- Reject cookies when asked (usually at the start of using a site for the first time).
- Delete cookies at the end of each session for social media, shopping, travel and health research.
- Use browser settings like "Delete cookies on exit."
- For very sensitive activities, use a temporary container or a private window (e.g. FireFox + Containers).

Remember: Cookies = crumbs of your digital behaviour. Clearing them keeps the crumbs out of other people's hands.

Bonus: Improve Your Search Privacy

Even if you change browsers, your search engine still shapes your privacy experience.
Privacy-enhancing search engines:

- **DuckDuckGo** (independent alternative to Google)
- **Startpage** (no tracking, no search history)
- **Brave Search** (independent index)

Avoid Google/Bing and Safari where possible. They link search behaviour to identity and advertising networks.

Simple Three-Step Upgrade Plan

If all of this feels overwhelming, try this phased approach, which will reduce your exposure by 60–70%:

- Step 1: Install a browser that has a focus on privacy (LibreWolf, Mullvad, Firefox).
- Step 2: Add uBlock Origin and turn off all syncing.
- Step 3: Create a separate browser profile for banking and government services.

Get more resources & kit here: **www.MyResistKit.com**

ALIGNED COUNCIL OF AUSTRALIA

RCR .media