Browser Privacy Settings Tool

Tool · Configure Every Browser You Use For Maximum Privacy.

A per-browser audit tool that walks you through the exact privacy toggles in Chrome, Firefox, Safari, Brave, and Edge. Tick each setting as you adjust it.

Chrome

- Settings → Privacy and security → Third-party cookies → 'Block third-party cookies.'
- Settings → Privacy and security → Send a 'Do Not Track' request → ON.
- Settings → Privacy and security → Site Settings → Notifications → 'Don't allow' (default).
- Settings → Privacy and security → Site Settings → Microphone / Camera → reviewed.
- Settings → Search engine → set to DuckDuckGo or Brave Search if maximum privacy desired.
- Settings → Sync and Google services → review what's synced. Disable Personalisation toggle.
- Extensions → Manage Extensions → remove any you don't actively use.

Firefox

- Settings → Privacy & Security → Enhanced Tracking Protection → 'Strict.'
- Settings → Privacy & Security → Cookies and Site Data → 'Cross-site tracking cookies and isolate other cross-site cookies.'
- Settings → Privacy & Security → 'Always send a Do Not Track signal' → ON.
- Settings → Privacy & Security → 'Tell websites not to sell or share my data' → ON.
- Settings → Privacy & Security → Permissions → Notifications/Camera/Mic/Location reviewed.
- about:config → privacy.resistFingerprinting → true (advanced users).
- Extensions → uBlock Origin installed.

Safari

- Safari → Settings → Privacy → Prevent cross-site tracking → ON.
- Safari → Settings → Privacy → Hide IP address → 'From trackers and websites' (iCloud+).
- Safari → Settings → Privacy → Manage Website Data → cleared.
- Safari → Settings → Search → 'Show Suggestions' / 'Preload Top Hit' → consider OFF.
- Safari → Settings → Websites → Camera/Microphone/Location → review per-site.

Brave

- Settings → Shields → Trackers and ads blocking → 'Aggressive.'
- Settings → Shields → Block fingerprinting → 'Standard' or 'Aggressive.'
- Settings → Shields → Cookie blocking → 'Block third-party cookies.'
- Settings → Privacy and security → 'Send a Do Not Track request' → ON.
- Settings → Search engine → defaults already privacy-respecting.

Edge

- Settings → Privacy, search, and services → Tracking prevention → 'Strict.'
- Settings → Privacy, search, and services → Send 'Do Not Track' requests → ON.
- Settings → Privacy, search, and services → 'Always use Strict tracking prevention when browsing InPrivate' → ON.
- Settings → Privacy, search, and services → Manage permissions → reviewed.

Universal Add-Ons

- **uBlock Origin** — blocks 90% of trackers automatically. Free, open-source.
- **Privacy Badger** — EFF's tracker-blocker, complementary to uBlock.
- **Tampermonkey + 'Bypass Paywalls Clean'** — for paywalled news (legal, ethical use only).
- **Decentraleyes** — serves common CDN files locally instead of from Google/Cloudflare.