Browser & App Privacy Settings Cheat Sheet

Overview

Use this as a quick privacy audit. You don’t need to do everything at once — pick a section and knock out a few items. Revisit every few months.

Browsers

Firefox

- Turn on Enhanced Tracking Protection: **Strict**.
- Auto-clear cookies and history on close (Settings → Privacy & Security).
- Enable HTTPS-Only Mode (Settings → Privacy & Security → HTTPS-Only Mode → “Enable in all windows”).
- Install privacy extensions: uBlock Origin, Privacy Badger, Decentraleyes.

Brave

- Ensure Shields are enabled (blocks ads, trackers, cookies by default).
- Disable fingerprinting where possible (Settings → Shields).
- Use Brave’s password manager, or disable it and use an external manager consistently.

Chrome / Edge

If you must use Chromium browsers, tighten privacy settings and add blockers.

- Turn on “Block third-party cookies”.
- Disable “Preload pages for faster browsing” (can leak browsing habits).
- Enable HTTPS-First mode (Settings → Privacy & Security → Security).
- Add extensions like uBlock Origin and Privacy Badger.

Tor Browser

- Download only from torproject.org.
- Use HTTPS versions of sites when possible.
- Avoid logging into accounts tied to your real identity if anonymity is the goal.
- Do not install extra extensions (they can weaken anonymity).

General browser privacy tips

- Keep your browser updated.
- Block or limit third-party cookies.
- Clear browsing history and cache regularly (or auto-clear on close).
- Use HTTPS whenever possible.
- Limit permissions like microphone, camera, or location unless truly needed.

Mobile

iOS (iPhone / iPad)

- Settings → Privacy & Security → Location Services: set most apps to “While Using” or “Never”.
- Settings → Safari: enable “Prevent Cross-Site Tracking”.
- Settings → Privacy & Security → Apple Advertising: turn off “Personalized Ads”.
- Keep iOS updated regularly.

Android

- Settings → Location: set apps to “Only while using” or revoke entirely.
- Settings → Privacy: turn off “Usage & diagnostics” where possible.
- Google settings → Ads: opt out of Ads Personalization.
- Use privacy-respecting apps from **F-Droid** when possible.

General mobile privacy tips

- Review app permissions every few months.
- Keep your operating system and apps updated.
- Turn off background activity for apps that don’t need it.
- Disable microphone, camera, or location access by default; allow case-by-case.

Messaging Apps

WhatsApp

- Settings → Privacy: Last Seen & Online → My Contacts (or Nobody).
- Turn off Read Receipts if you prefer more control.
- Enable Two-Step Verification.

Signal

- Settings → Privacy: enable “Always relay calls” for extra anonymity.
- Enable “Screen security” to block screenshots inside the app (where supported).

Telegram

- Settings → Privacy: Last Seen & Online → Nobody.
- Disable “People nearby”.
- Turn on auto-delete messages for private chats when appropriate.

Session Messenger

- No phone number required: your Session ID is your identity.
- End-to-end encrypted by default, routed through decentralized infrastructure.

- Enable disappearing messages for sensitive chats.
- Prefer Session over SMS for private conversations.

General messaging privacy tips

- Prefer end-to-end encrypted apps.
- Turn off read receipts if you want more control.
- Regularly clear old chats and backups.
- Use disappearing messages for sensitive conversations.
- Avoid SMS for anything private — it is not secure.

Social Media

Facebook

- Settings → Privacy: “Who can see your friends list” → Only Me.
- Turn off face recognition (if available in your region).
- Disable location history and background location access.
- Review Off-Facebook Activity and clear it.

Instagram

- Switch to a private account.
- Turn off activity status (“Show when you’re active”).
- Disable location access at the device level.

Twitter / X

- Settings → Privacy & Safety: protect your posts.
- Turn off personalization based on inferred identity (where available).
- Disable location sharing in posts.

TikTok

- Settings → Privacy: disable “Suggest your account to others” if you want more privacy.
- Disable location services at the device level.
- Restrict third-party data sharing in privacy settings where possible.

Bluesky

- Adjust who can reply to your posts in settings.
- Limit discoverability if you do not want algorithmic promotion.
- Use moderation tools proactively (mute, block, filters).
- Review connected apps and revoke access you do not use.

General social media privacy tips

- Avoid posting real-time locations.
- Use different usernames across platforms when possible.
- Be cautious accepting random friend/follow requests.
- Regularly review connected apps and third-party logins.
- Limit visibility of birthdates, family details, and personal info.

Quick Wins Checklist

- Block third-party cookies in your browser.
- Set location access to “While Using” for most apps.
- Clear cookies/history automatically.
- Turn off personalized ads and ad tracking.
- Enable HTTPS-Only / HTTPS-First mode in browsers.
- Disable cross-site tracking (especially on mobile).
- Prefer encrypted messengers like Signal or Session.
- Lock down social media visibility and disable location sharing.