Ximy

Everyday Privacy

A Simple Guide

Contents

Introduction

Every day we use technology that makes life easier. Maps that get us there, chats that keep us close, photos that save our memories, tap-to-pay that speeds us through the day. That convenience is real. But it isn't free. We pay for ease with pieces of ourselves: our clicks, locations, contacts, and habits. Over time, a second version of you is built on servers; an ad profile, a movement pattern, a social graph, shaping what you see, what you're offered, and sometimes what you believe.

This guide won't tell you to go off-grid or stop using the tools you love. Instead, it gives you a few simple moves that return control without breaking your routine. We start where you feel it most; social media, private messages, and the ads that follow you. Then we shore up the foundations: stronger passwords, cleaner accounts, safer photos and files, healthier devices, and small habits that stick.

Take this one step at a time. Even a couple of changes will cut the noise, reduce risk if something goes wrong, and make your digital life feel calmer. Privacy isn't about hiding; it's about choosing what to share, with whom, and for how long, so your technology serves you, not the other way around.

Section 1 Limit Social Media Exposure

Social keeps you connected, but small “breadcrumbs” (venue tags, skyline angles, logos, routine posts) can map your life.

Post smarter

Delay posts. Share after you leave. Tag wider areas. “Paris” > exact venue. Vary routines. Don’t broadcast the same time/place weekly. Keep captions vague while you’re there; add details later (optional).

Watch the frame

Crop/blur storefronts, building numbers, school/work logos, badges, boarding passes, wristbands, QR codes, room/cabin numbers. Mind window views that pinpoint your building. Protect kids’ identifiers (uniforms, school names, name labels).

Tighten settings:

1. Turn off Precise Location for social apps; remove photo location before posting.
2. Disable contact syncing.

Platform quick wins:

- *Instagram:* Private or Close Friends; Activity Status OFF; tag/mention approval ON; prevent story resharing.
- *TikTok:* Limit comments/duets/stitches; Downloads OFF.
- *Facebook:* Default = Friends; Tag/Timeline Review ON; Face recognition OFF; Limit past posts.

Trips & events

1. Post trips after you’re back.
2. Never share boarding passes/QR codes.
3. At festivals/cruises, crop wristbands and cabin numbers.

Two-minute setup

1. Private (or Close Friends).
2. Precise Location OFF; contact syncing OFF.
3. Tag/mention approval ON.

Section 2 Protect Your Chats & Calls

Not all messengers protect you equally; backups and lock-screens are common leaks.

Safer defaults

Use Signal (best all-round) or iMessage (Apple-to-Apple). Avoid SMS for anything sensitive.

Quick hardening

Disappearing messages for sensitive chats. Hide lock-screen previews. Short auto-lock (1–2 min) + PIN/biometric. Be careful with links; prefer in-app calls over cellular when privacy matters.

Backups (the gotcha)

- iMessage: Consider Advanced Data Protection.
- Signal: Local encrypted backups only (opt-in).
  If a backup isn't end-to-end encrypted, treat it as readable.

Identity & number

- Verify safety codes in Signal for key contacts.
- Set a carrier PIN
- Move 2FA from SMS → authenticator app/security key.

Groups & files

- Share like it could be forwarded.
- Use admin-only invites; review members.
- Strip photo metadata; use view-once for sensitive items.

Travel/Wi-Fi

Prefer mobile data; on public Wi-Fi, keep apps updated and use a trusted VPN like ProtonVPN.

Note: Using mobile data allows your ISP to see unencrypted data going through your phone

Minimal routine

1. Use Signal (or iMessage).
2. Encrypt/disable chat backups.
3. Authenticator app for 2FA.
4. Disappearing messages + no lock-screen previews.

Section 3 Browsers & Search Engines: Stop Feeding the Ad Machine

Your browser is the biggest data faucet. Shut most of it with a few defaults.

60-second setup

1. **Block third-party cookies.**
2. **Force HTTPS.**
3. Install **uBlock Origin** (optionally Privacy Badger/ClearURLs).
4. **Turn off ad personalization** (Google/Apple/Meta).
5. **Use separate browser profiles** (work / personal / banking).
6. **Sign out of Google** in your general-browsing profile.

Good defaults

Firefox for desktop (with Total Cookie Protection)
Firefox Focus for mobile.
Chrome/Edge work if you harden them.

Harden quickly

Firefox: Privacy = **Strict**; HTTPS-Only; uBlock; **Multi-Account Containers**.

Chrome: Block third-party cookies; Always use secure connections; uBlock; disable "payment methods" check.

Edge: Tracking prevention **Strict**; clear data on close; uBlock.

Search

Default to **DuckDuckGo**/**Startpage**. Use Google in a **separate profile** if needed.

Isolation

Keep a banking-only browser/profile.

Use profiles/containers to stop cross-site identity bleed.

Habits

Incognito hides local history, **not** you online. Review site permissions (camera/mic/location/notifications). Update browser automatically.

Optional: **DNS-over-HTTPS**; **Tor Browser** for sensitive research (slower, very private).

Section 4 Passwords & 2FA

Two moves stop most account takeovers: a **password manager** + **2FA**.

Password manager

Pick one: Bitwarden, 1Password, KeePass (offline).
Pick Proton Pass if you absolutely must use a cloud based password manager.
Generate one long passphrase (4–5 random words).
Enable PIN or biometric unlock.
Let it generate unique 20+ char passwords.
Never reuse passwords.

2FA priorities

1. Email
2. Bank/finance
3. Password manager
4. Apple/Google/Microsoft
5. Social/work

Best methods for 2FA

- **Security key** (FIDO2/WebAuthn) → strongest.
- **Authenticator app** (TOTP) → great default.
- **SMS** → last resort.

Don’t lock yourself out

Save backup codes offline; add a recovery email with 2FA.
Set carrier PIN (SIM-swap defense).

Monthly

Run manager’s Security Report; fix weak/reused passwords; close or randomize old accounts.

Section 5 Keep Your Accounts Separate

Limit blast radius with light compartmentalization.

Four buckets

1. Personal
2. Finance & ID
3. Work/School
4. Shopping/Newsletters

Easy separation

Email aliases: name+finance@..., name+work@..., name+shopping@...
Distinct usernames per bucket.
Optional second number for low-risk sign-ups; keep your main number for banking and family.

Sign-in choices

Prefer email + password over “Continue with...”. If you must use social sign-in, confine it to one bucket and a separate profile.

Recovery

Dedicated recovery email (used for nothing else) with 2FA. Store backup codes; keep a private note of what secures what.

Profiles/devices

- Banking-only browser/profile; separate work vs personal profiles.
- Disable contact syncing in social/shopping apps.

Monthly

Revoke old connected apps; turn off unneeded syncing; tidy newsletters.

Section 6 Hide Metadata in Files & Photos

Files carry hidden data (location, author, device). Remove it before sharing.

Phones

Turn off camera location (or at least Precise Location). Share without location; many apps offer this. Screenshots drop GPS but still reveal status bars; crop them.

Photo workflow

Crop/blur badges, numbers, logos, QR/barcodes. Strip EXIF (built-in options or a simple EXIF remover).

Documents/PDFs

Office: Inspect Document (remove author/company/hidden data).
PDFs: use real redaction; or Print/Export to PDF from a clean copy; check properties after.

Never post

Boarding passes
Event QR codes
ID barcodes
Legal documents

10-second check

1. Location stripped?
2. Identifiers hidden?
3. Author info removed?
4. Right audience?

Section 7 Clean Up Your Devices

Make devices boring targets and easy to recover.

5-minute setup

Step 1: Strong lock (PIN/biometric); auto-lock 1–2 min; hide message previews.

Step 2: Find My ON + remote wipe enabled.

Step 3: Full-disk encryption (FileVault/BitLocker; iPhone/modern Android default).

Step 4: Auto-updates ON for OS & apps. *(If you insist on manual, set a weekly reminder—e.g., Sun 16:00.)*

Step 5: Backups: ON and protected by 2FA; keep recovery codes somewhere safe.App & network hygiene

Step 6: Delete unused apps; review permissions (Location/Camera/Mic/Contacts = Ask/While Using).

Step 7: Public Wi-Fi → prefer mobile data; otherwise use a trusted VPN like Proton VPN.

Step 8: AirDrop/Nearby Share: keep Off by default; when needed, set to Contacts Only.

Step 9: Turn off auto-join for public networks; forget old café/airport Wi-Fi.

Laptop specifics

1. Use a standard user daily (save admin for installs/settings).
2. Learn the lock shortcut (Win+L / Ctrl+Cmd+Q).
3. Keep a banking-only browser/profile; clear Downloads/Desktop regularly.

Mobile specifics

4. SIM PIN + carrier account PIN (SIM-swap defense).
5. Limit lock-screen previews for sensitive apps.
6. Be cautious with “unlock with watch” if it’s too permissive.

If lost:
Locate → Mark as Lost → Remote wipe → Change email/bank passwords → Revoke sessions (Google/Apple/Microsoft + socials).

Monthly Check(3 min)

Make sure you have updates installed, permissions reviewed, apps cleaned up, backups verified, “Find My” still working.

Section 8 Small Habits = Big Privacy Wins

Tiny defaults that add up.

Every day (seconds)

Step 1: Pause before links/attachments.

Step 2: Lock your screen when you stand up.

Step 3: Share to small audiences first.

Step 4: Let the password manager create passwords.

Step 5: Tap **Don't Allow** on permissions you don't need.

Weekly (2–5 min)

Inbox sweep; one-in/one-out apps; browser tidy; install updates.

Monthly (10 min)

Password manager Security Report; 2FA on new accounts; revoke old app connections; permissions review; sign out old sessions.

Set-and-forget

1. Ad personalization OFF; auto-delete activity (3–18 months).
2. Banking-only browser/profile.
3. Contact syncing OFF for social apps.
4. Breach alerts ON for your primary email.

10-second sharing check

Audience right?
Location delayed?
Identifiers hidden?
Future-you okay with it?

Bonus: Test Yourself

Do this in 10–15 minutes; repeat monthly.

1. **Browser (3 min):** Test at amiunique.org or coveryourtracks.eff.org. Confirm: third-party cookies blocked, HTTPS forced, uBlock installed. Set private search.
2. **Passwords & 2FA (3 min):** Fix reused/weak passwords; 2FA on Email/Bank/Apple-Google-Microsoft; save backup codes.
3. **Social (3 min):** Private/Close Friends; Precise Location OFF; Activity Status OFF; tag/mention review ON; contact syncing OFF; post after leaving.
4. **Devices (3 min):** Auto-lock 1–2 min; previews hidden; Find My ON; erase option present; backups + 2FA.
5. **Metadata (2 min):** Remove photo location; inspect docs; export clean PDFs.

Score 1 point per "Pass."
4–5: solid

2–3: tighten

0–1: revisit Sections 3–7.

Conclusion

You don't need to disappear, just set better defaults. Post later. Harden your browser. Use a password manager with 2FA. Separate accounts. Clean metadata. Lock, update, and back up devices. Keep small habits.

You live in two places; in the world and in the servers. You can't control everything online, but you can control what you share, who sees it, and how long it sticks.

If you do only three things now:

1. Install uBlock Origin, block third-party cookies, set a private search.
2. Move logins into a password manager and enable 2FA on email and banking.
3. Make social accounts private, turn Precise Location OFF, and approve tags/mentions.

Then run the Bonus: Test Yourself monthly. Your footprint shrinks; your peace of mind grows. Privacy isn't about hiding; it's about choosing.