Sentrly

The 30-Minute Privacy Setup Checklist

Stay private online. Without the marketing fluff.

What this is. A practical setup checklist you can complete in 30 minutes to materially improve your online privacy and security. Every step is free, vendor-neutral, and explained without jargon.

Who it's for. Anyone who's been meaning to 'get serious' about privacy but never knew where to start. No technical background required.

How to use it. Print this PDF or keep it on screen. Work through the steps in order. Each section has clear instructions, an estimate, and a why-this-matters note.

Last updated: 2026-05-02 · Reviewed by Lena Park, Cybersecurity Editor

Step 1 — Browser hardening (5 min)

Why: Most online tracking happens in the browser. Switching browser or installing one extension stops the majority of consumer-grade tracking instantly.

■ Switch to Brave or Firefox (Strict mode) as your default browser

■ Install uBlock Origin extension

■ In Firefox: settings → Privacy & Security → Strict tracking

■ Block third-party cookies (browser settings)

■ Enable Global Privacy Control

Step 2 — Encrypted DNS (5 min)

Why: Stops your ISP from logging every site you visit. Configure once at the router and every device on your network is protected.

■ Pick a resolver: Cloudflare 1.1.1.1, NextDNS, or Quad9

■ Configure on your router (best) or per-device

■ Verify at dnscheck.tools that change took effect

Step 3 — Phishing-resistant 2FA on critical accounts (10 min)

Why: Email is the recovery channel for everything. Protecting it stops 99% of automated account takeover attempts.

■ Enable passkeys on Google: g.co/passkeys

■ Enable passkeys on Apple, Microsoft, GitHub, your password manager

■ For accounts without passkeys: install authenticator app (Aegis, 2FAS, Raivo)

■ Disable SMS as primary 2FA where stronger options work

■ Save backup codes in a sealed envelope at home

Step 4 — Password manager (5 min to set up, ongoing benefit)

Why: Unique strong passwords on every account stop credential-stuffing attacks. Manual memorization can't scale; a manager solves this.

■ Install Bitwarden (free) or 1Password ($36/year)

■ Set master passphrase: 5-7 random words

■ Write master passphrase on paper, store in a safe

■ Set up emergency access (designated trusted contact)

■ Migrate email + banking passwords first

Step 5 — Mobile privacy (3 min)

Why: Apps track you across the day via your advertising ID. Disabling it severs cross-app behavioral profiling.

■ iOS: Settings → Privacy & Security → Apple Advertising → Off

■ iOS: Settings → Privacy → Tracking → 'Allow Apps to Request to Track' Off

■ Android: Settings → Google → Ads → Delete advertising ID

■ Audit installed apps; remove ones you haven't used in 60 days

Step 6 — Auto-updates everywhere (2 min)

Why: Most consumer breaches exploit known vulnerabilities for which patches were available. Auto-updates close that window automatically.

■ Enable iOS / Android automatic OS updates

■ Enable Windows Update / macOS automatic updates

■ Enable browser automatic updates (most are on by default)

■ Restart browser daily so pending updates apply

■ Check router firmware update once per quarter

After the 30 minutes

Once you've completed Steps 1-6, your everyday privacy and security baseline is well above 90% of internet users. The remaining gains come from habits, not one-time setup:

• **Hover every link before clicking.** The link text can lie; the actual destination domain doesn't.

• **Verify sensitive requests out-of-band.** Any email asking for credentials, payment, or account changes — call the sender on a known number to verify.

• **Audit OAuth-connected apps quarterly.** Google: myaccount.google.com → Security. Microsoft: account.microsoft.com → Privacy.

• **Watch for breach alerts.** haveibeenpwned.com — set up notifications for your email addresses.

• **Review bank statements monthly.** Card-not-present fraud often starts with $1-3 test charges.

If you only do three things…

Phishing-resistant 2FA on email + a password manager + auto-updates everywhere. These three close roughly 85% of consumer breach impact paths.