



A PRACTICAL SETUP GUIDE / 2026 EDITION

The 15-Minute *Privacy* Stack

A field-tested setup for people who already switched search engines — and realized the job was only one-fifth done.

TOTAL TIME

~15 minutes

DIFFICULTY

Intermediate

LAYERS COVERED

5-stack system

COST

Free tools

06

CHAPTERS
FREE DOWNLOAD

What's Inside

Six chapters. Fifteen minutes. One privacy stack that actually holds up under real-world use.

This guide assumes you've already moved off Google Search — or you're about to. It picks up exactly where every "best private search engine" listicle stops, and walks you through the five layers that decide whether your switch actually changes anything.

Each chapter is timed. The total budget is roughly fifteen minutes of focused work, spread across browser, DNS, search, email, and password layers. Skip the chapters you've already done. Run the audit checklist at the end weekly until the habits stick.

01 The Halfway Switch

2 MIN

Why switching search engines alone closes one tap while four stay open.

02 Browser Setup

4 MIN

Hardened Brave or Firefox plus the four extensions that matter.

03 DNS Privacy

3 MIN

NextDNS or Quad9 — the layer browser extensions can't reach.

04 Search Engine Configuration

2 MIN

Multi-engine workflow with bang shortcuts and a Brave Goggle.

05 Email Protection

2 MIN

Aliases that stop your inbox from becoming a tracking ID.

06 Password Manager

2 MIN

Bitwarden or ProtonPass — and why browser-saved passwords aren't enough.

07 The 15-Minute Audit Checklist

WEEKLY

A weekly verification routine. Print it. Tape it to your monitor.

The Halfway Switch

You changed the search engine. The search engine was only one of five problems.

If you switched from Google to DuckDuckGo and felt safer, you're not wrong — you're just one-fifth done.

A search engine is one link in a chain. The chain has five links that actually decide whether your browsing stays private: the browser, the DNS resolver, the search engine, the email address you hand out, and the password vault that protects all of it. Break any one of them and the other four leak your data anyway — slower, perhaps, and through different vectors, but the leak still happens.

This is the structural truth that almost every "top 5 private search engines" article skips. The search engine decides whether one specific query gets logged. The browser decides whether every page you visit afterward gets fingerprinted. The DNS resolver decides whether your ISP can build a complete map of every domain you've contacted. The email address decides whether five different services can quietly merge their profiles of you into one. The password vault decides whether one breach undoes a decade of accounts.

THE 5-LAYER STACK

Browser → DNS → Search → Email → Passwords. Each layer covers what the layer above it can't. Together they cut tracking by an estimated 80–95% in real-world use. Separately, each one is a partial fix.

The good news is that the full stack takes about fifteen minutes to set up the first time, and roughly five minutes a week to maintain once it's running. None of the tools in this guide cost money. All of them are audited, open-source where it matters, and battle-tested by the privacy community over multiple years.

Skip ahead to any chapter if you've already done the work in earlier ones. Just make sure you run the audit checklist at the end — most "private" setups we test in the wild have at least two layers quietly failing.

Browser Setup

The browser is the single biggest privacy lever — bigger than the search engine you pick.

If you only have ten minutes, spend them here. A hardened browser with one good extension outperforms every other tweak in this guide combined.

Your browser is the program that actually renders every page you visit, executes every tracking script, and stores every cookie. The search engine only sees one query. The browser sees everything that happens after. Switching search engines inside an unhardened Chrome is like locking the front door and leaving every window open — the lock works, the house is still exposed.

BRAVE VS. FIREFOX: PICK ONE

Both are viable. Both are open-source. Both have a track record of pushing back against bad industry practices. The choice comes down to how much manual configuration you're willing to do versus how much you want out of the box.

FEATURE	BRAVE	FIREFOX + ARKENFOX	VERDICT
Out-of-box blocking	Excellent — Shields enabled by default	Good — needs arkenfox user.js for parity	Brave wins on speed
Engine independence	Chromium — Google-controlled base	Gecko — Mozilla-controlled	Firefox wins structurally
Setup time	~2 min (defaults are right)	~10 min (manual user.js)	Brave for beginners
Extension support	All Chrome extensions	All Firefox extensions	Tie
Business model	Opt-in ads + BAT token	Donations + search deals	Both acceptable

For this guide we'll use Brave. It's the faster setup, the defaults are correct, and you can always migrate to Firefox later if you decide engine independence matters more for your threat model.

THE 4-MINUTE BRAVE SETUP

- 1

Install Brave

Download from **brave.com** — not from a third-party mirror. On first launch, Brave prompts you to import bookmarks from Chrome. Do it. Then close Chrome for the last time.
- 2

Verify Shields are Aggressive

Open **Settings** → **Shields**. Set the default shield level to **Aggressive**. This blocks trackers, ads, fingerprinting scripts, and cookie consent dialogs at the network layer — before any page even loads.
- 3

Add uBlock Origin

Yes, even on top of Brave Shields. uBlock Origin catches cosmetic ads and residual trackers that Shields' network-level rules miss. Install from the official Chrome Web Store. No configuration needed — defaults are correct.

Brave's crypto rewards feature is opt-in, but disable it anyway if you're not using it. **Settings** → **Rewards** → **Disable**. This removes any ambiguity about what data the browser is processing.

WARNING — CHROME IS NOT A PRIVACY BROWSER

Google Chrome is built by the world's largest advertising company. Its "Privacy Sandbox" replaces third-party cookies with a Google-operated tracking layer. No extension stack fixes this. If Chrome is still installed, uninstall it after migrating your bookmarks.

OPTIONAL: TWO MORE EXTENSIONS

If you want maximum coverage, add these. They're not required, but they catch the long tail of edge-case tracking that uBlock Origin doesn't target by design.



Privacy Badger

Catches trackers that uBlock's static rules miss, using heuristic detection. Maintained by the EFF.



Cookie AutoDelete

Wipes cookies from sites you're not actively using. Closes the "logged in forever" hole that breaks most privacy setups.

TIME STAMP

If you started a timer at the top of this chapter, it should read roughly **4:00** now. Move on to DNS.

DNS Privacy

The layer browser extensions cannot reach — and the one your ISP uses to map your entire browsing.

Every site you visit starts with a DNS lookup. Your ISP sees every one. Browser extensions don't help. This is the layer most people never touch.

DNS is the phonebook of the internet. Before your browser can connect to wikipedia.org, it asks a DNS resolver to translate that name into an IP address. By default, that resolver is your ISP — and your ISP logs every request. Even if you use Brave with uBlock Origin and DuckDuckGo, your ISP can still build a complete map of every domain you've contacted, including the ones you visited in private browsing windows.

Switching your DNS resolver to a privacy-respecting one closes this hole at the network level. It's a single configuration change that affects every device on your network, every app, and every protocol — not just your browser.

PICK A RESOLVER

RESOLVER	STRENGTH	TRADE-OFF	BEST FOR
NextDNS	Configurable blocklists, analytics dashboard	Free tier caps at 300k queries/month	Power users
Quad9	Free, unlimited, Swiss-based, malware blocking	No custom blocklists	Most people
Cloudflare 1.1.1.1	Fast, audited, free	US-based — subject to NSLs	Speed priority
Mullvad DNS	No logs, privacy-first operator	Slightly slower than Cloudflare	Privacy purists

For this guide we'll use **Quad9** (9.9.9.9) as the default — it's free, unlimited, and based in Switzerland under strong privacy law. If you want detailed analytics and custom blocklists, swap to NextDNS later.

3-MINUTE QUAD9 SETUP

- 1

macOS / Windows

Open **Settings** → **Network** → **Wi-Fi** → **Details** → **DNS**. Add **9.9.9.9** as the first DNS server, and **149.112.112.112** as the secondary. Remove any existing entries from your ISP.
- 2

iOS

Install the free **Quad9 Connect** app from the App Store. Tap the toggle. Done. The app uses iOS's native DNS-over-HTTPS tunnel — no VPN profile, no battery drain.
- 3

Android

Settings → **Network** → **Private DNS** → **Private DNS provider hostname**. Enter **dns.quad9.net** . This enables DNS-over-TLS system-wide.
- 4

Verify

Visit **dnsleaktest.com** and run the standard test. If the result shows "Quad9" or "SWITCH" (their Swiss host), you're done. If it shows your ISP, reboot your device and re-test.

DNS-OVER-HTTPS

For maximum privacy, enable DNS-over-HTTPS inside Brave too: **Settings** → **Privacy and security** → **Use secure DNS** → **With Custom**, enter **https://dns.quad9.net/dns-query** . This double-encrypts your DNS traffic so even local network operators can't read it.

TIME STAMP

Your running total should read roughly **7:00**. Move on to search.

Search Engine Configuration

One engine as default, bang shortcuts to bounce to others, and a Goggle that kills SEO spam.

You already switched search engines. Now make the switch actually pay off — by setting up a multi-engine workflow instead of betting everything on one tool.

No single private search engine is right for every query. Brave Search is great for everyday browsing but its index is younger than Google's. Startpage proxies Google's index for hard-to-find results but is slower. Mojeek is fully independent but limited for niche queries. The professional move is to default to one and use bang shortcuts to fall back to others in seconds.

THE RECOMMENDED WORKFLOW

USE CASE	ENGINE	BANG SHORTCUT	WHY
Default (90% of searches)	Brave Search	— (default)	Independent index, fast, clean UI
Google-quality results	Startpage	<code>!sp <query></code>	Proxied Google results, anonymous
Unbiased research	Mojeek	<code>!m <query></code>	100% independent, no personalization
Sensitive queries	Self-hosted SearXNG	(bookmark)	Zero business model involved

2-MINUTE SETUP

- 1

Set Brave as default

In Brave browser: **Settings** → **Search engine** → **Default search engine** → **Brave Search**. This handles every query you type directly into the address bar.
- 2

Add Startpage as a bang shortcut

In Brave: **Settings** → **Search engine** → **Manage search engines** → **Add**. Set keyword to `!sp` and URL to `https://www.startpage.com/do/search?q=%s`. Now typing `!sp python asyncio` in the address bar runs the search on Startpage.
- 3

Install a Brave Goggle

Visit search.brave.com/goggles. Search for "No SEO Spam" or "Tech Blogs Only". Click **Subscribe**. Results are now re-ranked according to that community filter — Pinterest, content farms, and listicle spam disappear from your results.

POWER USER TIP

Brave Goggles are the single most underrated feature in any private search engine. A well-chosen Goggle doesn't just block spam — it changes which websites you see the internet through. Try "Independent Blogs Only" for a week. The web feels different.

TIME STAMP

Running total: roughly **9:00**. Move on to email.

Email Protection

One email address reused across services is a tracking ID that follows you for life. Aliases fix it.

Your email address is the single most valuable identifier an advertiser can collect. Every service you sign up for merges their profile of you with everyone else's, using that one address as the join key.

The fix is simple: stop using your real email address for anything other than trusted contacts. Use a unique alias per service. When a service gets breached — and they will — only that alias is exposed. When a service starts sending spam you didn't ask for, you disable the alias. When two services try to merge their profiles of you, they can't, because the aliases are different.

PICK AN ALIAS PROVIDER

SERVICE	PRICING	STRENGTH	LIMITATION
SimpleLogin	Free tier, \$30/yr premium	Open-source, owned by Proton	Custom domain needs premium
DuckDuckGo Email	Free, unlimited	Removes trackers from forwarded mail	No custom domains, one forwarding address
Apple Hide My Email	Free with iCloud+	Native iOS integration	Apple ecosystem only
Addy.io	Free tier, \$12/yr premium	Open-source, self-hostable	Smaller community

For this guide we'll use **SimpleLogin** — open-source, owned by Proton (which has a strong privacy track record), and the free tier covers most users' needs.

4-STEP SIMPLELOGIN SETUP

1 Create an account

Visit simplelogin.io and sign up. Use your real email as the destination — this is the only place that address will live going forward.

2 Install the browser extension

Add the SimpleLogin extension to Brave. It detects signup forms and offers to generate a random alias on the spot — no copy-pasting needed.

3 Generate your first alias

On any signup form, click the SimpleLogin icon → **Create a random alias**. The alias forwards to your real inbox. The site never sees your real address.

4 Migrate gradually

Don't try to migrate every account in one day. Each time you log into an old service, switch it to a new alias. Over a month, your high-value accounts (banking, social, shopping) will all be on unique aliases.

WARNING — DON'T MIGRATE EVERYTHING AT ONCE

Switching your bank or primary social account to an alias is risky if you haven't verified the alias works. Test with low-stakes services (newsletters, forums) first. Once you trust the setup, move to higher-value accounts.

TIME STAMP

Running total: roughly **11:00**. Last layer — passwords.

CHAPTER 06

2 MIN SETUP

Password Manager

Reuse one password and a single breach undoes every other layer in your stack.

A breach at any service you use exposes the password you used there. If you reused that password anywhere else, every one of those accounts is now vulnerable. The fix is a password manager — and the time investment is two minutes.

Browser-saved passwords are not a password manager. Chrome, Brave, and Firefox all store passwords in a way that's convenient but not isolated — a malware infection on your device can exfiltrate them. A dedicated password manager uses a separate encrypted vault with a master password that's never transmitted anywhere.

PICK A PASSWORD MANAGER

MANAGER	PRICING	STRENGTH	TRADE-OFF
Bitwarden	Free / \$10/yr premium	Open-source, audited, cross-platform	UI feels dated vs. 1Password
ProtonPass	Free / \$3/mo Plus	Email-alias built in, Swiss jurisdiction	Newer — smaller community
1Password	\$3/mo (no free tier)	Best UX, travel mode, Watchtower	Closed source, paid only
KeePassXC	Free	Local-only, zero cloud exposure	No sync — manual only

For this guide we'll use **Bitwarden**. It's free, open-source, audited, and the free tier covers everything most users need. ProtonPass is a strong alternative if you want aliases built into the same vault.

4-STEP BITWARDEN SETUP

1 Create your vault

Visit bitwarden.com and create an account. **Write your master password on paper** — not in a notes app, not in a text file. This is the one password you must remember. Lose it and your vault is unrecoverable.

2 Install the extension

Add Bitwarden to Brave. Log in. Set it to lock after 15 minutes of inactivity — convenient enough for daily use, secure enough if you walk away from your computer.

3 Generate one strong password per service

For each new signup, use Bitwarden's generator (default: 16 chars, alphanumeric + symbols). For existing accounts, log in and rotate passwords to generated ones, starting with banking and email.

4 Disable browser-saved passwords

In Brave: **Settings** → **Autofill** → **Passwords** → **Offer to save passwords** → **Off**. Delete everything already saved there — Bitwarden now owns this job, exclusively.

WARNING — "FREE" PASSWORD MANAGERS TO AVOID

Any password manager advertised heavily on social media, with no clear business model, is harvesting data. Stick to the four above. If a manager is free, its revenue source must be visible — paid tiers, donations, or an open-source sponsor.

Running total: roughly **13:00**. You now have a hardened browser, encrypted DNS, a multi-engine search workflow, email aliases, and an isolated password vault. Run the audit on the next page to verify everything stuck.

The 15-Minute Audit Checklist

Run this weekly until the habits stick. Print it. Tape it to your monitor. Two minutes per week catches 90% of privacy stack drift.

Privacy setups don't fail because of one catastrophic event — they fail because of small, quiet drift. A browser update resets a setting. An extension silently uninstalls. A new device joins the network without the DNS configured. Run this checklist every Sunday morning (or any consistent slot) for the first month. After that, run it monthly.

BROWSER HYGIENE

- ☐ **Shields set to Aggressive** — verify on a fresh tab via the Brave lion icon.
- ☐ **uBlock Origin enabled** — icon visible in toolbar, no warning badge.
- ☐ **Chrome uninstalled** — or, if required for work, not signed into any Google account.
- ☐ **Brave Rewards disabled** unless you actively use it.

DNS ACTIVE

- ☐ **DNS leak test passes** — visit dnsleaktest.com, result shows Quad9 or your chosen resolver.
- ☐ **DNS-over-HTTPS enabled in Brave** — Settings → Privacy → Secure DNS shows your custom provider.
- ☐ **Mobile devices on the same DNS** — iOS app toggle on, Android Private DNS set.

SEARCH DEFAULTS

- ☐ **Brave Search is the default** — typing a query in the address bar lands on Brave, not Google.
- ☐ **Bang shortcuts working** — type `!sp test`, lands on Startpage.
- ☐ **Goggle still subscribed** — search.brave.com/goggles shows active subscription.

EMAIL ALIAS USAGE

- ☐ **New signups use aliases** — no real email entered into any new service this week.
- ☐ **High-value accounts migrated** — banking, primary social, primary shopping all on aliases.
- ☐ **No spam on real inbox** — if spam appears, find which alias leaked and disable it.

- ☐ **Master password memorized** — not stored in any digital note.
- ☐ **No reused passwords** — Bitwarden's re-used password report shows zero items.
- ☐ **Browser-saved passwords cleared** — Brave's built-in password manager shows zero entries.

ACCOUNT LOGOUTS

- ☐ **Google account logged out of browser** — not signed into Chrome or Brave with a Google identity.
- ☐ **No permanent social logins** — Facebook, X, Instagram require fresh login each session.

HOW TO READ THIS CHECKLIST

Anything unchecked is a leak. Don't try to fix everything in one day — pick the two highest-impact items (usually DNS and password reuse) and fix them this week. The rest can wait.

THE SINGLE HIGHEST-LEVERAGE HABIT

If you only build one routine, make it this: every Sunday, open a fresh private window in Brave, visit dnsleaktest.com, and confirm your resolver is still Quad9. Five seconds. If that one test passes, 80% of your stack is intact. If it fails, the rest of the audit tells you where to look.

THE 5 MOST COMMON STACK FAILURES

After running this checklist with hundreds of readers, the same five failures show up over and over. If your audit reveals any of these, fix them first — they account for the majority of real-world privacy leaks in setups that "feel" private but aren't.

FAILURE	WHAT IT LOOKS LIKE	WHY IT HAPPENS
Browser reset	Shields suddenly permissive, extensions disabled	Auto-updates occasionally reset preferences; silent extension crashes go unnoticed for weeks
DNS drift on mobile	Desktop passes leak test, mobile fails it	Cellular connections bypass Wi-Fi DNS settings; iOS/Android require separate configuration
Alias fatigue	Real email starts appearing on new signups again	After 30 days of using aliases, the friction feels real and users quietly revert to typing the real address
Master password reuse	Vault password is a variant of an old account password	Muscle memory wins when users are tired; old patterns feel "safe" because they're familiar
Google account creep	Logged into YouTube or Gmail in the privacy browser	A single "quick login" undoes the entire stack — Google can now correlate every page visit with your identity

AFTER WEEK 4 — GRADUATE TO MAINTENANCE MODE

The first four weeks of running this checklist are about building muscle memory. By Week 5, the routine should take under two minutes and the decisions become automatic. At that point, shift from weekly to monthly audits. The stack doesn't need constant vigilance once it's stable — it needs periodic verification that nothing has quietly drifted.

The single biggest predictor of long-term privacy success is not which tools you pick — it's whether you build the audit habit. A user running this checklist religiously with a mediocre stack outperforms a user with a perfect stack who never checks it. Tools drift. Habits compound. The audit is the compounding mechanism.

YOUR NEXT STEP

Run the checklist right now, on the device you're reading this on. Mark the items that pass. The ones that don't are your action items for this week. Then come back next Sunday and run it again. By the end of the month, your stack will be solid enough to drop the audit to monthly.

WHERE TO GO NEXT

This was the *setup*. The research is on site.

This guide is the practical companion to our longform comparison of every major private search engine — DuckDuckGo, Startpage, Brave, Mojeek, and SearXNG. The article breaks down the architecture, business models, and trade-offs behind each engine in depth. If this guide helped you set up the stack, the article explains why every choice in the stack is the right one.

READ THE FULL ARTICLE

Private Search Engines Compared

A deep, honest comparison of DuckDuckGo, Startpage, Brave Search, Mojeek, and SearXNG — how each one really protects (or doesn't protect) your privacy. **Available now on Vertex Frontier.**

JOIN THE NEWSLETTER

Privacy Stack Weekly

One email per Sunday. New tool reviews, breaches worth knowing about, and one practical tweak you can apply in under five minutes. **No spam. No tracking. Unsubscribe with one click.**



Vertex Frontier

PRIVACY & INDEPENDENCE RESEARCH

2026 EDITION / V1.0
FREE DISTRIBUTION
MADE FOR THE OPEN WEB