BEFORE YOU START

Quick Wins:
Do These This Weekend

Before we jump into the deep end here — phones, network setup, custom ROMs — I want to give you super quick changes to make ASAP. The following five changes take between fifteen minutes and an hour each, require no technical knowledge, and will meaningfully reduce your data exposure the second you implement them.

This is your first step. Pick one. Do it. The momentum matters more than the order.

From

The Privacy Diet

James Patrick

1
WIN

Switch Your Browser

⏱ 15 min ★ Impact: High

Your browser is the window through which you do almost everything online. Chrome, which most people use by default, is made by Google — whose entire business model is built on knowing what you do online. Using Chrome is like hiring Google to sit beside you and take notes every time you use the internet.

The fix is simple: install a privacy-respecting browser and make it your default. You keep all your usual websites. You lose the surveillance.

Recommended:

> **Brave** — Built-in ad and tracker blocking, Chromium-based so familiar if you're coming from Chrome. Zero setup required. My pick for most people.

> **Firefox** — Open source, highly customisable, massive privacy extension ecosystem. The best choice if you'd rather avoid Chromium.

First thing to do after installing:

- Install uBlock Origin (the single most effective privacy tool available as a browser extension)
- Set it as your default browser in your OS settings
- Never open Chrome again (or delete it — you won't miss it)

2
WIN

Switch Your Search Engine

⏱ 5 min ★ Impact: High

Google Search is not neutral. It tracks every query you make, builds a profile of your interests, fears, and intentions, and uses that data to target advertising. Beyond privacy, there's a subtler problem: your results are personalised to you, which means two people searching for the same thing may get very different answers. Your search engine is shaping your reality.

The switch costs you nothing but a few seconds of habit adjustment.

Recommended:

> **Startpage** — Fetches Google results without sending Google your identity. Best of both worlds if you're attached to Google's results quality.

> **DuckDuckGo** — Independent index, no tracking, excellent !bang shortcuts. My daily driver.

> **Brave Search** — Fully independent index, no reliance on Google or Bing at all. Growing fast.

Set your chosen search engine as default in your new browser's settings. Takes thirty seconds. Done.

3
WIN

Audit and Lock Down Your App Permissions

⏱ 30 min ★ Impact: High

Most people have apps on their phone that have been quietly harvesting data for years — location, microphone, contacts, camera — because they clicked "Allow" once at installation and forgot about it. Go through your phone right now and review what you've permitted.

On iPhone:

- Settings → Privacy & Security → Location Services
- Review every app. Ask: does this app genuinely need my location?
- Repeat for Microphone, Camera, Contacts, and Photos

On Android:

- Settings → Privacy → Permission Manager
- Browse by permission type (Location, Microphone, Camera, etc.)
- Revoke anything that doesn't make sense. A flashlight app has no business knowing your location.

The rule of thumb:

If you can't immediately explain why an app needs a given permission, revoke it. Most apps work perfectly fine without the data they've been quietly collecting.

4

WIN

Install a Password Manager

⏱ 45 min ★ Impact: Critical

If you reuse passwords — and if you're not using a password manager, you almost certainly do — you are one data breach away from losing access to everything. This is not a privacy issue, it's a security issue, and security is the foundation on which all privacy rests. A compromised account leaks data in ways no amount of privacy tooling can prevent.

A password manager generates and stores a unique, strong password for every account you have. You remember one master password. It handles the rest.

Recommended:

> **Bitwarden** — Open source, free tier is excellent, can be self-hosted if you want full control. My recommendation for most people.

> **KeePassXC** — Fully local, no cloud, no account required. Maximum control. Slightly more setup involved.

Getting started takes 45 minutes: install, import any saved browser passwords, and start replacing weak/reused passwords as you log into things over the next week. You don't need to change everything at once.

While you're here — enable two-factor authentication (2FA) on your most important accounts:

Email account (your most critical account — everything resets through it)

Banking and financial accounts (most already force 2FA)

Password manager itself (critical: 2FA and very good passphrase/master password)

Use an authenticator app (FreeOTP+,Aegis on Android, 2FAS or Ente Auth on iOS) rather than SMS codes — SIM-swapping attacks make SMS 2FA weaker than it looks.

NOTE: have you been part of a data breach already? Check Have I been Pwned?

5
WIN

Switch Your Messaging App

⏱ 15 min ★ Impact: High

WhatsApp is owned by Meta. Your messages are end-to-end encrypted, yes — but your metadata is not. Meta knows who you talk to, how often, for how long, at what times, and from where. That metadata is often more revealing than the message content itself. SMS is even worse: unencrypted, carrier-logged, trivially interceptable.

The alternative is Signal. It is the gold standard for private messaging — end-to-end encrypted, open source, independently audited, collects almost no metadata, and used by journalists, lawyers, security researchers, and privacy-conscious civilians worldwide. It looks and works almost identically to WhatsApp.

How to make the switch:

- Download Signal (free, iOS and Android)
- Message your five most-contacted people and ask them to install it
- Move your most sensitive conversations there first
- Expand from there at your own pace

You can keep WhatsApp for the contacts who won't switch. But moving even your closest relationships to Signal significantly reduces your metadata exposure.

Your Weekend Checklist

Here's the full list at a glance. Tick them off as you go:

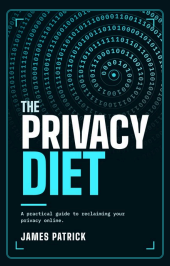
	Task	Time
☐	Switch to Firefox or Brave, install uBlock Origin	**15 min**
☐	Set DuckDuckGo, Startpage, or Brave Search as default	**5 min**
☐	Audit app permissions on your phone	**30 min**
☐	Install Bitwarden or KeePassXC, enable 2FA on email	**45 min**
☐	Download Signal, invite your key contacts	**15 min**

Total time: Under two hours. These five changes alone put you ahead of the vast majority of internet users. Everything in the rest of this guide builds from here.

Go one step further: an always-on VPN

These five changes plus an always-on VPN put you further ahead still. With a VPN running all the time, your internet provider can no longer see which sites you visit, people on the same public Wi-Fi can't watch your traffic, and websites see the VPN's address instead of yours.

Choose a paid provider with an independently audited no-logs policy (the book recommends Mullvad or ProtonVPN), never a free VPN, and turn on its auto-connect or always-on setting. A VPN doesn't make you anonymous: it moves your trust from your internet provider to the VPN provider. Chapter 6 of *The Privacy Diet* explains what a VPN does and doesn't do.



This is where The Privacy Diet starts.

The book goes on through your phone, your browser and email, and your home network, with a complete checklist at the end.

Get the book on Amazon · **theprivacydiet.com**

The Quick Wins above are reproduced from *The Privacy Diet* by James Patrick.