# Beginner's Guide To Online Privacy

*Guide · What's Tracked, Who's Collecting It, And The Five Practical Defences That Actually Move The Needle.*

**Who this is for: anyone who feels surveilled but isn't sure which actions actually help. Privacy isn't all-or-nothing. This guide explains what's worth doing, what's overhyped, and the order to do things in.**

## Privacy Vs. Anonymity

Privacy is keeping ordinary information about you out of the hands of people who don't need it. Anonymity is being unidentifiable. Most people want privacy — they're fine with their bank knowing they bank there; they just don't want every advertiser, data broker, and stranger online knowing too. This guide focuses on privacy.

## What's Actually Being Collected

The data collected about you falls into five categories:

- **Behavioural data** — what you click, search, watch, and buy. Aggregated by ad networks across many sites.
- **Personal data** — name, address, age, family, income. Sold by data brokers to advertisers, employers, landlords.
- **Location data** — where you go, when. Collected by phone apps and aggregated.
- **Communication metadata** — who you email, who you text, who you call. Even when content is encrypted, the metadata reveals patterns.
- **Biometric data** — facial recognition, voice prints, fingerprints. Collected by phones, security systems, social-photo platforms.

## Who's Collecting It

| Actor | What They Want | How To Reduce Their Take |
|---|---|---|
| Big Tech (Google, Meta, Apple, Amazon) | Behavioural profile to sell ads | Reduce login footprint, opt out of tracking, use privacy-respecting alter |
| Your ISP | Browsing patterns; sometimes monetised | Use a VPN or DNS-level encryption (DoH). |
| Data brokers (Spokeo, BeenVerified, etc.) | Sell your personal info to anyone | Manual opt-outs or services like DeleteMe / Incogni / Optery. |
| Apps on your phone | Location, contacts, mic access, ad ID | Audit permissions; delete unused apps; reset Ad ID. |
| Sites you visit | Cookies, fingerprints, return visits | Strict tracking protection; ad blocker; private browsing. |

# The 5 Defences That Actually Help

## 1. Use A Privacy-Respecting Browser With Tracking Protection

Default Chrome with default settings is the worst privacy environment. Switch to Firefox (with Strict tracking protection), Brave, or Safari (with Privacy Protection). Add uBlock Origin. This single change blocks ~90% of trackers and ad networks.

## 2. Email Aliases For Every New Signup

Every site you give your real email to becomes a node in a tracking graph that can match you across services. Use Apple's Hide My Email, SimpleLogin, Firefox Relay, or DuckDuckGo Email Protection. Each service gets a unique alias that forwards to your real address. Compromised aliases can be deleted instantly without affecting your real email.

## 3. Audit Phone Permissions Quarterly

Most apps don't need location, microphone, contacts, or photo access. Open Settings → Privacy and review every permission. Set anything you don't actively need to 'While Using' or 'Never.' iOS 14+ and Android 12+ both make this easy.

## 4. Opt Out Of Data Brokers

Data brokers collect your name, address, age, family, income — then sell it. Manual opt-outs are free but slow (30-60 minutes per broker, 50+ brokers exist). Services like DeleteMe / Incogni / Optery automate the process for $50-150/year. Worth it for most people.

## 5. Reduce Big-Tech Footprint

Big Tech is the largest single source of behavioural data about you. The most realistic step isn't quitting them — it's reducing what they collect:

- **Google:** myactivity.google.com → turn off Web & App Activity, Location History, YouTube History.
- **Meta:** Settings → Privacy Centre → Off-Facebook Activity → Disconnect.
- **Apple:** Settings → Privacy & Security → Tracking → toggle off 'Allow apps to request to track.'
- **Amazon:** Your Account → Advertising Preferences → opt out.

# VPNs, Demystified

VPNs encrypt traffic between your device and a VPN server. They hide your IP from the sites you visit and your traffic from your local network (coffee-shop Wi-Fi, hotels). They do NOT make you anonymous, do NOT stop tracking by Google or Facebook, and do NOT prevent malware. Use a VPN on public Wi-Fi or when you don't trust your ISP. Avoid free VPNs — they monetise by selling your data.

# Quick Wins You Can Do Today

1. Install uBlock Origin in your browser. (5 min)
2. Set up Hide My Email or SimpleLogin. (10 min)
3. Audit phone permissions. (10 min)
4. Sign up for DeleteMe / Incogni / Optery — or pick 5 brokers and opt out manually. (1 hour)

5 Turn off Google Web & App Activity. (2 min)

## Where To Go Next

- **Run the Privacy Lockdown Workbook** — comprehensive privacy reset.
- **Run the Privacy Reset Checklist** — 15-minute weekly reset.
- **Use the Browser Privacy Settings Tool** — exact settings per browser.
- **Read the Data Privacy Cheat Sheet** — quick reference for who tracks what.