DIGITALLY UNDRESSED

FREE TOOLKIT

Advanced Overwatch

Browser hardening, DNS protection, permission auditing, and network-level defense

You have done the basics. This guide goes deeper - into the network-level, browser-level, and system-level protections that block tracking before it reaches your device. Written for people ready to take the next step, explained so anyone can follow along.

Estimated time: 30-45 minutes

From the book *Why Am I the Only One Naked?*

thedreamerai.com/digitally-undressed

Share this guide freely. Privacy is not a privilege.

Part 1: DNS-Level Protection

Every time you visit a website, your device asks a DNS server "where is this site?" By default, that question goes to your internet provider - who logs it, can sell it, and can be compelled to hand it over. Changing your DNS is like choosing a different phone book operator - one that does not record what you look up.

[Step 1] Change Your DNS Provider

Choose a provider:

- **Cloudflare (1.1.1.1):** Fast, privacy-focused, does not log identifying queries. Install the 1.1.1.1 app on iPhone or Android for one-tap setup. Simplest option.
- **NextDNS:** Customizable. Blocks ads, trackers, and malware at the DNS level before they reach your browser. Free tier covers 300,000 queries/month (enough for most people). Best option for power users.
- **Quad9 (9.9.9.9):** Non-profit. Blocks known malicious domains automatically. No account needed. Just set DNS to 9.9.9.9. Best "set and forget" option.

How to set it up:

- **iPhone:** Settings > Wi-Fi > tap your network > Configure DNS > Manual > delete existing servers > add 1.1.1.1 and 1.0.0.1 (or your chosen provider). For system-wide coverage including cellular: install the 1.1.1.1 app or set up a DNS profile.
- **Android:** Settings > Network & Internet > Private DNS > enter "one.one.one.one" (Cloudflare) or your provider's hostname.
- **Router (protects every device):** Log into your router admin page (usually 192.168.1.1 or 192.168.0.1). Find DNS settings under WAN or Internet. Replace ISP DNS with your chosen provider. This protects every device on your network - including smart TVs, speakers, and IoT devices you cannot configure individually.

> **PRO TIP**
> NextDNS with a custom blocklist can block Facebook tracking, Google Analytics, and ad networks across your entire home network before they ever load. It is the most powerful single change in this guide.

> **IMPORTANT**
> Do not use Google DNS (8.8.8.8) for privacy. It is fast, but Google logs all queries. Using Google DNS to protect privacy from Google is like asking the fox to guard the henhouse.

Part 2: Browser Hardening

Your browser is the single most intimate piece of software on your device. It sees your medical searches, financial concerns, relationship questions, and late-night curiosities. Hardening it means reducing what it tells websites about you.

[Step 2] Essential Browser Extensions

- **uBlock Origin** (Firefox, Chrome, Edge): Open-source ad and tracker blocker. The gold standard. Blocks ads, trackers, and malicious scripts. Free, no data collection. Note: Google's Manifest V3 transition may limit uBlock Origin on Chrome - Firefox remains the most reliable platform for this extension.
- **Privacy Badger** (Firefox, Chrome, Edge): Made by the Electronic Frontier Foundation. Learns to block invisible trackers as you browse. Complements uBlock Origin - use both together.
- **Cookie AutoDelete** (Firefox, Chrome): Automatically deletes cookies when you close a tab. Whitelist sites you want to stay logged into. Deletes tracking cookies from everywhere else.
- **For Safari users:** Safari has strong built-in tracking protection. Add the 1Blocker or AdGuard extension from the App Store for additional coverage.

> **IMPORTANT**
> Do not install more than 4-5 extensions. Each extension can see your browsing data. Stick to open-source, well-established extensions with large user bases and transparent privacy policies.

[Step 3] Browser Fingerprinting Protection

- **What fingerprinting is:** Even without cookies, websites can identify you by combining your screen resolution, installed fonts, timezone, browser version, graphics card, and dozens of other signals into a unique "fingerprint." This works in incognito mode and across sessions.
- **Firefox:** Settings > Privacy & Security > Enhanced Tracking Protection > Strict. Firefox in Strict mode blocks most known fingerprinting techniques automatically.
- **Brave Browser:** Blocks fingerprinting by default. Randomizes fingerprintable signals so your browser looks different to every site. Strongest out-of-the-box privacy browser available.
- **Test yourself:** Visit coveryourtracks.eff.org (EFF). It shows how unique your browser fingerprint is and exactly what makes it identifiable. Run the test before and after changes to see the improvement.

> **PRO TIP**
> Using a common browser (Firefox) with common settings makes you less fingerprintable than an exotic setup. You blend into the crowd. Privacy through uniformity.

Part 3: The Full Permission Audit

Your phone has a permission system controlling which apps can access your camera, microphone, contacts, photos, health data, and more. Most people grant permissions during install and never revisit them.

[Step 4] Camera and Microphone

- **iPhone:** Settings > Privacy & Security > Microphone. Review every app. If it does not need your microphone to function, revoke access. Repeat for Camera.
- **Android:** Settings > Privacy > Permission Manager > Microphone. Same process. Repeat for Camera.
- **What to keep:** Video calling apps (Zoom, FaceTime, Teams), voice recorders, camera apps. That is the complete list. Your weather app does not need your microphone. Your shopping app does not need your camera.
- **The myth debunked:** "My phone is listening to me." Most apps are not actively listening through the microphone - they do not need to. Your search history, location data, and purchase patterns predict your interests more accurately than eavesdropping. The targeting feels like listening because the data is that good.

[Step 5] Contacts and Photos

- **Contacts:** When an app accesses your contacts, it gets names, phone numbers, email addresses, and sometimes physical addresses for everyone in your phone. That is not just your data to share - it belongs to every person in your address book.
- **Review contacts access:** iPhone: Settings > Privacy & Security > Contacts. Android: Settings > Privacy > Permission Manager > Contacts. Revoke aggressively.
- **Photos:** On iPhone, you can grant "Selected Photos" access instead of full library. When an app asks for photo access, choose "Select Photos" and give it only what it needs.
- **What your photos contain:** GPS coordinates, timestamps, device information, faces, text in images. Your photo library is a detailed record of where you were, who you were with, and what you were doing - with dates attached.

> **CRITICAL**
> Social media apps that request contacts access upload your entire address book to their servers. Facebook, Instagram, TikTok, and Snapchat all do this. Once uploaded, your contacts' information exists on their servers permanently - even if you later revoke access.

[Step 6] Connected Apps and OAuth Tokens

- **What these are:** Every time you click "Sign in with Google" or "Continue with Facebook," you grant that service ongoing access to your account. These connections persist until you manually revoke them - even if you stop using the app.
- **Google:** myaccount.google.com > Security > "Third-party apps with account access" > remove anything unrecognized or unused.
- **Apple:** Settings > [Your Name] > Sign-In & Security > "Sign in with Apple" > review and revoke.
- **Facebook:** Settings > Apps and Websites > review and remove.
- **X (Twitter):** Settings > Security and Account Access > Apps and Sessions > Connected Apps.

> **PRO TIP**
> Do this quarterly. Apps you connected once and forgot about still have active access to your data until you explicitly revoke them. Calendar reminder. Every three months.

Part 4: Network-Level Protection

[Step 7] VPN Usage - When It Actually Matters

- **What a VPN does:** Encrypts traffic between your device and the VPN server. Your ISP cannot see what sites you visit. Public Wi-Fi snooping is blocked.
- **What a VPN does NOT do:** Make you anonymous. Block ads. Protect you from phishing. Prevent websites from tracking you through cookies or fingerprinting. A VPN is one layer, not a silver bullet.
- **When to use one:** Public Wi-Fi (coffee shops, airports, hotels). When you do not want your ISP logging your browsing. When accessing content restricted by location.
- **Recommended:** Mullvad (anonymous signup, no email required, $5/month, audited). ProtonVPN (free tier available, Swiss jurisdiction, open-source). IVPN (transparent, privacy-audited, multi-hop).
- **What to avoid:** Any free VPN not from a known privacy organization. Free VPNs typically monetize by logging and selling your traffic - the exact opposite of their marketing promise.

> **IMPORTANT**
> Do not use a VPN for banking unless you consistently connect from the same server region. Banks flag VPN connections as suspicious activity and may lock your account.

[Step 8] Email Aliasing

- **What it is:** Instead of giving your real email to every website, give each one a unique alias that forwards to your real inbox. If an alias starts getting spam, you know exactly who sold your address - and you kill that alias without affecting anything else.
- **SimpleLogin** (free tier: 10 aliases): Open source. Integrates with ProtonMail. Acquired by Proton in 2022 - backed by a privacy-focused company.
- **Apple Hide My Email:** Built into iCloud+ ($0.99/month). Works natively across all Apple devices. Easiest option for Apple users.
- **Firefox Relay** (free tier: 5 aliases): Made by Mozilla. Simple browser extension generates aliases on the fly.
- **Real-world use:** Sign up for a store's newsletter with store-name@youralias.com. When that address starts getting spam from unrelated senders, you know the store sold your data. Kill the alias. Problem contained.

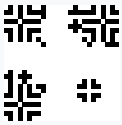
> **PRO TIP**
> Use a unique alias for every online account. It is the simplest way to trace who sells your data and to contain breaches to a single alias instead of your entire digital identity.

What You Have Built

You now have layered defenses working at every level of your digital life.

DNS-level blocking stops trackers before they reach your browser. Browser hardening blocks what gets through. Permission auditing limits what apps can access on your device. Network protection encrypts your traffic in transit. Email aliasing compartmentalizes your identity across services.

No single layer is perfect. That is the point. Security works in layers - each one catches what the others miss. You are not paranoid. You are informed. And that is the most dangerous thing you can be to a company that profits from your ignorance.



Want the full architecture of surveillance?

Why Am I the Only One Naked? exposes the business models, data flows, and tracking techniques behind 50 platforms - graded, explained, and fixed.

Free with Kindle Unlimited.

Scan the QR code or visit amazon.com/dp/B0DQJPPKGM