Privacy Focused

This document contains all the blog posts from https://privacy.celestial.dev/

You can download your own version by going to the website and clicking the Download button or by visiting: https://privacy.celestial.dev/download/blog.pdf

Hope this helps someone!

Escape Launcher: A Minimal Android Home Screen

February 17, 2026

Your phone's home screen is designed to grab your attention. Icons, notifications, widgets—everything competing for your eyes. Escape Launcher does the opposite: it makes your phone boring on purpose.

What Is It?

Escape Launcher is a minimal Android launcher that strips away visual stimulation. Instead of colorful icons arranged in a grid, you get a simple text list of your daily apps.

The interface:

- Home screen shows a text list of apps you use regularly
- No icons, no widgets, no visual clutter
- Swipe right to access your full app list
- That's it

The goal is simple: reduce the urge to pick up your phone and scroll mindlessly. When opening your phone isn't visually rewarding, you do it less.

Why This Helps

It breaks the habit loop - Most phone checking is automatic. You unlock, scan for notifications or interesting icons, and get pulled into apps. Escape Launcher removes the visual triggers that start this cycle.

Makes intentional use easier - When you need a specific app, you find it in the list. When you're just bored, there's nothing to catch your eye. Your phone becomes a tool again, not an entertainment device.

Reduces context switching - Fewer visual distractions mean less temptation to jump between apps. You open what you need, use it, and put the phone down.

This won't work for everyone. Some people need visual organization. But if you're fighting phone addiction, removing visual stimulation helps.

The Privacy Angle

Most launchers in the Google Play Store track you. They log:

- Which apps you open and when
- How long you spend on your home screen
- What you search for in app drawers
- Your usage patterns over time

This data goes back to the launcher company and often gets sold to advertisers or data brokers.

Escape Launcher doesn't track anything. It's fully open-source, available on F-Droid and GitHub, with no analytics built in. You can verify this yourself by reviewing the source code at https://github.com/GeorgeClensy/Escape-Launcher.

No telemetry, no accounts, no data collection. It's just a launcher.

How to Use It

Installation:

1. Download from F-Droid or build from source on GitHub
2. Install like any other app
3. Open the new app and set it as your default launcher when prompted

Setup:

- Choose which apps appear on your home screen list
- Swipe right to see all installed apps

- That's the entire configuration

You can switch back to your old launcher anytime through Android settings. Nothing is permanent.

What You're Trading

No widgets - If you rely on weather, calendar, or quick-info widgets, this won't work for you.

No visual organization - Icon placement and folders help some people find apps quickly. Text lists are slower for visual thinkers.

Learning curve - You need to remember app names instead of recognizing icons. This takes adjustment.

Limited customization - Escape Launcher is minimal by design. If you want themes, icon packs, or heavy customization, look elsewhere.

This launcher isn't for power users who want extensive features. It's for people trying to use their phone less.

Who This Is For

Escape Launcher works well if you:

- Check your phone compulsively without purpose
- Get distracted by notification badges and colorful icons
- Want to be more intentional about phone usage
- Value privacy and don't want your launcher tracking you
- Prefer function over aesthetics

It doesn't work well if you:

- Need quick access to many apps simultaneously
- Rely on widgets for information
- Organize spatially rather than textually
- Want a visually appealing home screen

Combining With Other Changes

A minimal launcher is most effective when paired with other adjustments:

- Turn off non-essential notifications
- Remove social media apps or move them off your home list
- Enable grayscale mode (makes your screen less appealing)
- Set app timers for problematic apps
- Keep your phone in another room at night

The launcher addresses visual triggers. You still need to handle behavioral patterns separately. If it doesn't help, switch back. If it does, keep using it. The point is finding what works for your habits, not following someone else's setup.

Small open-source projects come with trade-offs. Updates are slower, features are limited, and support is community-driven. But you get transparency and privacy in return. Don't download from unofficial sources. Stick to F-Droid or build it yourself to ensure you're getting the clean version.

Your phone should serve you, not the other way around. Sometimes that means making it less interesting to look at.

F-Droid - An Android App Store

February 13, 2026

The Play Store is the default on android devices, but it's not your only option on Android. F-Droid offers a different philosophy for app distribution. Here's what that means for you.

The Fundamental Difference

Google Play Store is a commercial marketplace. Google controls what gets listed, scans apps for malware, and tracks everything you do. They know what apps you download, when you use them, and tie that data to your Google account.

F-Droid is a catalog of free and open-source software (FOSS). Every app's source code is publicly available. F-Droid builds the apps themselves from that source code, so you know what you're getting matches what's published.

One is convenient and comprehensive. The other is transparent and privacy-focused.

What F-Droid Actually Offers

Open-source only - If the source code isn't public, it's not on F-Droid. This means you (or security researchers) can verify what an app actually does instead of trusting the developer's claims.

No tracking - F-Droid doesn't require an account. They don't log what you download or build profiles on you. The Play Store ties everything to your Google identity.

No proprietary libraries - Apps on F-Droid can't include Google's tracking frameworks or advertising SDKs. Many Play Store apps are free because they monetize your data. F-Droid apps can't do that.

Built by F-Droid - F-Droid compiles apps from source code on their own servers. This prevents developers from sneaking in malicious code that isn't in the public repository. The Play Store trusts developers to submit clean builds.

The Privacy Angle

Every time you use the Play Store, Google knows:

- What apps you browse
- What you download and install
- When you open apps (if you have Play Services)
- Your app usage patterns over time

F-Droid doesn't track any of this. Downloading an app is a simple file transfer with no account required.

But here's the caveat: Many apps still need Google Play Services to function properly. Even if you download apps through F-Droid, if those apps rely on Google's infrastructure, you're still in Google's ecosystem. F-Droid shows which apps are truly independent.

The Security Question

This is where it gets nuanced. **Security and privacy are different things**.

Play Store security:

- Google scans apps for malware automatically
- Developers are vetted (to some degree)
- Quick takedowns of malicious apps
- Large security team monitoring threats

F-Droid security:

- Apps are built from auditable source code
- Smaller team, slower response to threats
- Community review process
- Transparency over corporate oversight

F-Droid's strength is transparency — you can verify what you're running. The Play Store's strength is Google's security infrastructure. Neither is perfectly secure. Evaluate your own risk tolerance.

What You're Giving Up

Be realistic about F-Droid's limitations:

Smaller selection - Most commercial apps aren't open-source and won't be on F-Droid. No Instagram, Spotify, or Uber.

Older versions - F-Droid apps sometimes lag behind their Play Store counterparts because F-Droid rebuilds from source.

Less polish - Open-source apps are often built by volunteers. They may lack the features or interface design of commercial alternatives.

Manual updates - F-Droid can auto-update, but it's not as seamless as the Play Store's background process.

No paid apps - F-Droid is for free software only. Developers can accept donations, but there's no payment infrastructure.

Common F-Droid Apps

F-Droid has solid open-source alternatives for many common needs:

- **NewPipe** - YouTube client without ads or Google tracking
- **Signal** - Encrypted messaging (also on Play Store)
- **Organic Maps** - Offline navigation without tracking
- **Simple Mobile Tools** - Calendar, gallery, contacts apps without bloat
- **AntennaPod** - Podcast player
- **Aegis** - Two-factor authentication

These won't replace everything, but they cover core functionality without the privacy trade-offs.

Using Both Stores

You don't have to choose exclusively. Many people run both:

- F-Droid for apps where privacy matters or open-source alternatives exist
- Play Store for apps that require it (banking apps, work apps, commercial services)

This hybrid approach lets you reduce your Google footprint without completely abandoning convenience.

One warning: Installing apps from multiple sources increases your attack surface. Each store is a potential entry point for malicious software. Know what you're installing and from where.

How to Actually Use F-Droid

F-Droid isn't pre-installed. You download the F-Droid app from their website (search on a privacy focused search engine) and sideload it.

Android will warn you about installing apps from unknown sources. This is a legitimate security feature. You're bypassing Google's gatekeeping. Make sure you're downloading from the official F-Droid site.

Once installed, F-Droid works like any app store—browse, search, install. Updates are handled within the F-Droid app.

The Philosophical Question

This isn't just about apps. It's about who controls your device.

Google's ecosystem is convenient because they control everything. One account, seamless integration, automatic updates. The cost is total visibility into your digital life.

F-Droid represents an alternative where you have more control but bear more responsibility. You choose what to install, verify what you're running, and accept less convenience for more transparency.

Neither is objectively better. It depends on your priorities.

Do Your Homework

Before switching or supplementing with F-Droid:

- Read F-Droid's documentation on how they build and verify apps
- Check which apps you currently use have open-source alternatives
- Understand the security implications of sideloading apps
- Look into whether F-Droid fits your threat model

Don't just swap app stores because someone said it's more private. Understand what you're gaining and what you're losing.

Your phone is yours. Choose who gets to see what you do with it.

GrapheneOS: Taking Full Control of Your Android Phone

February 17, 2026

Stock Android phones come with Google baked into every layer. GrapheneOS strips that out and rebuilds Android with privacy and security as the foundation. Here's what that actually means.

What Is It?

GrapheneOS is a privacy and security-focused mobile operating system built on the Android Open Source Project (AOSP). It's designed exclusively for Google Pixel phones, using their hardware security features while removing Google's software.

Key differences from stock Android:

- No Google Services by default (no Play Store, Gmail, Maps)
- Hardened security with additional exploit protections
- Network and sensor permission controls
- No telemetry or data collection
- Sandboxed Google Play option (if you need it)
- Fully open-source and auditable

This isn't just "degoogled Android." GrapheneOS adds security layers that stock Android doesn't have.

Why Pixel Phones?

This seems contradictory—using Google hardware to escape Google software. But Pixel phones have the strongest hardware security in Android:

- Titan M security chip for verified boot
- Longest security update support
- Strong bootloader protections
- Hardware-backed encryption

GrapheneOS leverages this security while removing Google's tracking. You get the best hardware security available without Google controlling the software.

Other phones don't have these hardware protections or their bootloaders can't be relocked after installing custom ROMs, creating security vulnerabilities.

What You Gain

Complete Google removal - No Google account required. No Play Services constantly tracking your location, app usage, and behavior. Your phone doesn't phone home to Google every few minutes.

Enhanced security - GrapheneOS hardens Android with:

- Stricter memory protections against exploits
- More granular permission controls
- MAC address randomization per network
- Improved sandboxing for apps
- Faster security updates (often before stock Pixels)

Network permission toggle - You can deny apps network access entirely. Install an app but don't let it communicate with the internet. Stock Android can't do this without root access or third-party tools.

Sensor permissions - Control access to sensors like accelerometer and gyroscope. These can be used for fingerprinting or tracking even when location is denied.

No bloatware - Carrier apps, manufacturer apps, and Google apps aren't installed. You start with a clean system and add only what you need.

Real control - You decide what runs on your device. No forced updates, no pre-installed apps you can't remove, no services running in the background without your knowledge.

The Google Play Compatibility Layer

GrapheneOS offers sandboxed Google Play Services. This is optional but important:

- You can install Play Store apps that require Google Services
- Play Services run as regular apps without special privileges
- You control their permissions like any other app
- They can't see other apps or system-wide data

This means you can run banking apps, work apps, or other software that requires Play Services without giving Google full system access. It's a middle ground between full degoogling and stock Android.

What You're Giving Up

Be realistic about the trade-offs:

Setup complexity - Installing GrapheneOS requires:

- Unlocking your bootloader
- Flashing system images from a computer
- Following technical instructions carefully
- Accepting that you could brick your device if done wrong

This isn't one-click installation. You need to be comfortable with command-line tools.

Banking and payment apps - Some apps detect unlocked bootloaders or custom ROMs and refuse to run. Google Wallet and some banking apps may not work even with sandboxed Play Services.

Convenience features - No Google Assistant, no automatic photo backup to Google Photos, no seamless integration with Google services. Everything that "just works" on stock Android requires manual setup.

Smaller app ecosystem - Without Play Store by default, you rely on F-Droid or sideloading. Many commercial apps aren't available outside Google's ecosystem.

Support burden - You're responsible for maintenance. No carrier support, no manufacturer warranty for software issues. The GrapheneOS community helps, but you're largely on your own.

Learning curve - Understanding how to use the enhanced security features, configure sandboxed Play, and troubleshoot issues takes time.

Who Should Use GrapheneOS

This makes sense if you:

- Have serious privacy concerns about Google's data collection
- Understand basic command-line operations
- Can troubleshoot technical issues independently
- Don't rely heavily on apps that refuse to run on custom ROMs
- Value control over convenience
- Already own or are willing to buy a supported Pixel device

This doesn't make sense if you:

- Want something that just works out of the box
- Rely on apps that detect and block custom ROMs
- Need Google's ecosystem integration for work or personal use
- Aren't comfortable with technical installation processes
- Want manufacturer support when things go wrong

Installation Basics

Installing GrapheneOS involves:

1. Buying a supported Pixel phone (check https://grapheneos.org/ for current list)
2. Backing up your data

3. Unlocking the bootloader through developer settings
4. Using the web installer or command-line tools to flash GrapheneOS
5. Relocking the bootloader for verified boot security
6. Setting up your apps and accounts

The GrapheneOS website has detailed installation instructions. Follow them exactly. Missing steps or doing them out of order can cause problems.

Critical: Unlocking your bootloader wipes your device completely. Back up everything first.

Daily Usage Reality

After installation, GrapheneOS works like Android with key differences:

App installation:

- F-Droid for open-source apps
- Aurora Store (anonymous Play Store access) for commercial apps
- Direct APK installation for anything else
- Sandboxed Play if you need Play Services

Updates:

- GrapheneOS updates over-the-air like stock Android
- Often faster security updates than Google provides
- You control when updates install

Performance:

- Generally as fast or faster than stock (less background processes)
- Better battery life (no Google Services draining power)
- More storage (no pre-installed bloat)

Privacy vs Security Again

GrapheneOS improves both, but understand the difference:

Privacy - Google can't track you because their services aren't running. Apps have fewer permissions by default. Your data stays on your device.

Security - Hardened system protections make exploits harder. Hardware security features remain active. Sandboxing is stronger.

Stock Android is secure but not private. GrapheneOS is both secure *and* private.

The Broader Context

Installing GrapheneOS doesn't eliminate all tracking:

- Cell towers still know your location
- Your carrier logs connection data
- Apps you install may track you independently
- Websites track through browser fingerprinting
- Credit cards log purchases

GrapheneOS handles phone-level privacy and security. You need additional tools (VPNs, privacy browsers, payment methods) for comprehensive privacy.

Long-Term Commitment

Switching to GrapheneOS is a significant change:

- You'll spend hours setting up and configuring
- Some apps won't work no matter what you try
- You'll need to maintain the system yourself
- Updates require more attention than stock Android

This isn't something to try casually. It's a commitment to taking full responsibility for your device's operation.

Where to Learn More

- **Official site**: grapheneos.org for documentation and installation guides
- **Community**: GrapheneOS forum and Matrix channels for support
- **Device compatibility**: Check which Pixel models are currently supported
- **Privacy guides**: Read comparisons with other privacy-focused Android ROMs

Don't rely on this article alone. Read the official documentation, watch installation videos, and understand what you're getting into.

Do Your Research

GrapheneOS represents a fundamental shift in how you use your phone:

- Read independent security audits of GrapheneOS
- Look into alternative ROMs (CalyxOS, LineageOS) and compare features
- Check recent discussions about what works and what doesn't
- Verify that the apps you need daily will function

True privacy requires effort. GrapheneOS gives you the tools, but you have to do the work.

Brave Browser

February 13, 2026

Web browsers like Google Chrome and Microsoft Edge will track you by default. Brave Browser tries to block trackers and ads out of the box. Here's what that actually means for your web surfing:

What Brave Does Differently

Blocks ads and trackers by default - You don't need extensions or configuration. Open Brave, and it immediately stops third-party ads, tracking scripts, and fingerprinting attempts. Sites load faster and cleaner.

Built on Chromium - Brave uses the same engine as Chrome, so websites work the same way. You get Chrome's compatibility without Google's tracking. The chromium engine is open source itself and can be verified to be free of analytics and tracking software.

HTTPS everywhere - Brave automatically upgrades connections to HTTPS when available, protecting your data from being intercepted on the network.

Fingerprinting protection - Websites try to identify you through your browser configuration, fonts, and device characteristics. Brave randomizes or blocks these signals to make tracking harder.

No telemetry by default - Chrome sends usage data back to Google constantly. Brave doesn't collect browsing data unless you explicitly opt in.

The Ad Replacement Model

Here's where Brave gets controversial. They don't just block ads—they replace them with their own.

Brave Ads are opt-in privacy-respecting advertisements. If you enable them, you see occasional notifications and earn BAT (Basic Attention Token), Brave's cryptocurrency. You can tip content creators with these tokens or cash them out.

Critics argue Brave profits by blocking other people's ads and inserting their own. Supporters say it's a fairer model where users get compensated for their attention.

You can disable Brave Ads entirely and just use it as an ad blocker. Managing an application like this takes a lot of work. If you aren't paying for the product, you are more than likely the product. Utilizing Brave's ad network is a way to help support the maintainers without sacrificing too much of your privacy.

Privacy Features That Actually Matter

Shield settings - Brave's blocking is granular. You can control cookie blocking, fingerprinting protection, and script blocking on a per-site basis. Break a website? Adjust shields for that domain only.

Private windows with Tor - Brave integrates Tor routing for private browsing. Your traffic goes through the Tor network, hiding your IP address. This isn't perfect anonymity (browser fingerprinting still exists), but it's better than standard incognito mode.

Search engine flexibility - Brave doesn't force you into a specific search engine. Set it to DuckDuckGo, Startpage, or whatever you prefer. Default search is configurable and not tied to ad revenue deals like other browsers.

No cross-site tracking - Third-party cookies are blocked by default. Ad networks can't follow you across websites to build behavior profiles.

What You're Giving Up

Some sites break - Aggressive blocking means some websites don't work properly. You'll need to adjust shields or whitelist sites occasionally.

Cryptocurrency integration - BAT and wallet features are baked in. If you're not interested in crypto, this is bloat. You can ignore it, but it's there.

Smaller extension library - Brave uses Chrome extensions, but their own store is limited. You can add Chrome Web Store extensions manually, but it's an extra step.

Less mainstream support - Fewer users means fewer resources for troubleshooting and community support compared to Chrome or Firefox.

Trust in Brave Software - You're shifting trust from Google to Brave. Their business model is different, but you still need to trust them. Read their privacy policy and verify their claims.

Mobile Privacy

Brave on mobile (iOS and Android) blocks ads and trackers just like desktop. This is huge for mobile browsing where ads are intrusive and data-hungry.

Mobile-specific benefits:

- Pages load faster without ad scripts
- Uses less data (blocked content isn't downloaded)
- Battery lasts longer (fewer background processes)
- Cleaner reading experience

Mobile Safari and Chrome don't block ads by default. Brave does. That alone changes the mobile web experience.

Brave vs Firefox

Firefox also prioritizes privacy. Here's the practical difference:

Brave - Privacy by default, no configuration needed, Chromium-based compatibility, built-in ad blocking **Firefox** - More customizable, non-Chromium engine, requires extensions for best privacy, stronger open-source community

Both are solid privacy-focused options. Brave is easier out of the box. Firefox gives you more control with more effort.

Brave vs Chrome

Chrome is fast, polished, and integrated with Google services. It's also Google's data collection tool.

Why switch to Brave:

- Stop Google from tracking your browsing
- Block ads without extensions
- Same website compatibility
- Faster page loads (no ad scripts)

Why stay with Chrome:

- Seamless Google account integration
- Better extension ecosystem
- More familiar if you're already invested

If you use Google services heavily (Gmail, Drive, Photos), switching browsers doesn't eliminate Google tracking. They still see your activity through those services. Brave helps with general browsing privacy, not account-based tracking.

The Open-Source Question

Brave is open-source. You can review the code, verify claims, and see what data is collected. This transparency matters.

However, being open-source doesn't automatically mean secure or private. It means auditable. Independent security researchers need to actually audit the code, and you need to check if they have.

Don't assume open-source equals trustworthy. Verify through third-party audits and reviews.

Practical Steps to Switch

Switching browsers is straightforward:

1. Download Brave from their official site
2. Import bookmarks and passwords from your current browser
3. Set your preferred search engine

4. Configure shields based on your comfort level
5. Browse normally and adjust shields when sites break

Start with default settings. Only customize if you run into issues. The out-of-box configuration is solid for most people.

Does This Actually Improve Privacy?

Brave blocks a significant amount of tracking by default. That's a real improvement over Chrome or unmodified Safari.

But browser privacy is one piece of a larger puzzle:

- You're still tracked through logins (Google, Facebook accounts)
- Device fingerprinting can identify you across browsers
- Your ISP sees what domains you visit (use a VPN for that)
- Apps on your device track you outside the browser

Brave helps with web browsing privacy. It doesn't make you anonymous or invisible. Combine it with other privacy tools for better overall protection.

Do Your Research

Before switching:

- Read independent browser privacy tests and comparisons
- Check Brave's privacy policy for what they actually collect
- Look into recent controversies or issues (they've had some)
- Test it yourself for a week and see if it fits your workflow

Don't switch just because someone said it's better. Understand what you're getting and make an informed choice.

Privacy is about reducing your exposure, not eliminating it. Brave is a tool, not a shield.

Email

February 10, 2026

The Core Difference: You Pay, So Your Data Doesn't

Gmail is free because Google profits from your data. They scan your emails to build advertising profiles and feed their business model. Paid services like proton mail charges a subscription fee instead. This fundamental shift means your emails aren't being mined for profit.

The trade-off is simple: pay with money or pay with your privacy.

Privacy ≠ Security

This is critical to understand: **privacy and security are not the same thing**.

- **Security** protects your data from unauthorized access (hackers, breaches)
- **Privacy** protects your data from authorized access (the company itself, governments, advertisers)

Both Gmail and Proton have strong security. The difference is privacy. Gmail is secure but not private—Google has full access to your emails. Proton is both secure *and* private because even they can't read your messages.

The Downsides

Be realistic about the trade-offs:

- **It costs money** - Free tier is limited; useful features require paid plans
- **Less convenient** - Some integrations don't work as smoothly as Gmail's ecosystem
- **Smaller storage** - You get less space than Gmail's generous free allocation
- **Learning curve** - Encryption adds complexity, especially when emailing non-Proton users

Is It Worth It?

That depends on what you value. If you're comfortable with Google reading your emails in exchange for free service, Gmail works fine. If you'd rather pay to keep your communications private, a paid tool, or a self-hosted tool is a legitimate alternative.

What We Use

Like the VPN article, I also use Proton mail. It has several nice features:

End-to-end encryption - Your emails are encrypted on your device before they reach Proton's servers. Even Proton can't read them. Gmail encrypts in transit, but Google can still access the content.

Based in Switzerland - Proton operates under Swiss privacy laws, which are stronger than US regulations. They're not subject to the same data requests that US companies routinely comply with.

No tracking - Proton doesn't log your IP address by default or build profiles on you. Gmail tracks everything you do to improve their ad targeting.

Open source - Proton's code is publicly available for security researchers to audit. This transparency builds trust, though you'll need to verify this yourself if it matters to you.

Take the Next Step

Don't just take this at face value. Research any paid email client's privacy policy yourself. Look into how email encryption actually works. Compare what data Gmail collects versus what tools like Proton collects. Read independent security audits.

The choice to improve your digital privacy starts with understanding what you're actually getting. Do your homework, then decide if it's worth the switch.

Read More About Self Hosting:

Self Host Email Article Coming Soon

Privacy is a practice, not a product. Proton Mail is one tool, but your overall digital hygiene matters more than any single service.

How to Install Pi-hole on a Raspberry Pi

February 18, 2026

This guide walks through setting up Pi-hole on a Raspberry Pi to block ads and trackers across your entire home network. Follow these steps carefully.

What You'll Need

Hardware

- Raspberry Pi (any model—even a Pi Zero works)
- MicroSD card (8GB minimum, 16GB recommended)
- SD card to USB adapter (for flashing from your computer)
- Ethernet cable
- Power supply for the Raspberry Pi
- A Mac or Linux machine for the easiest possible setup. Windows can be difficult to work with. If you have a Windows machine, consider using a Linux Live Boot USB to prepare the SD card and ssh connection.

Software

- **Raspberry Pi OS 64-bit Lite** - Download from raspberrypi.com/software
- **Balena Etcher** - https://etcher.balena.io/ (for flashing the SD card). You can use any other tool that accomplishes the same task. This one is recommended by the Linux Mint team.

Prerequisites

- Basic command-line knowledge
- Access to your router's admin panel
- About 30-45 minutes (or four hours if you're me)

Step 1: Prepare the SD Card

Important: Disconnect from any VPN before starting. VPN connections can interfere with finding devices on your local network. It may also prevent you from accessing the Pi-hole web interface later. Make sure you're on the same local network as your Raspberry Pi.

Flash Raspberry Pi OS

1. Download Raspberry Pi OS 64-bit Lite from the official website
2. Download and install Balena Etcher from https://etcher.balena.io/
3. Insert your SD card into the USB adapter and connect it to your computer
4. Open Balena Etcher
5. Select the Raspberry Pi OS image file
6. Select your SD card as the target
7. Click "Flash" and wait for the process to complete

Enable SSH Access

After flashing completes, the SD card will remount. You need to enable SSH so you can access the Pi remotely:

1. Navigate to the boot partition of the SD card (it should be visible in your file manager)
    - Sometimes this doesn't work right on Windows. You may need to use a mac or figure out a way to load linux temporarily on your computer using a Live Boot USB Drive. If you have a Linux machine, you can use that to prepare the SD card.
2. Create a blank file named `ssh` (no file extension)

- On Linux/Mac: `touch ssh` in the boot directory
- On Windows: Create a new text file and remove the `.txt` extension entirely

Set Up Default User Credentials

Create a file named `userconf.txt` in the boot partition:

1. Open a terminal on your Mac or Linux machine (or use a terminal emulator on Windows)
    - If you don't have a terminal, you can probably generate an openssl password online, but be cautious about using online tools for password generation. If you do use an online tool, make sure it's reputable and secure. It's generally safer to generate the password hash locally on your machine.
2. Generate a password hash by running:

    ```
    echo 'yourpassword' | openssl passwd -6 -stdin
    ```

    Replace `yourpassword` with your actual desired password
3. Copy the hash that's output (it will look like `$6$random_characters...`)
4. Create `userconf.txt` in the boot partition
5. Add this line to the file:

```
pi:THE_HASH_YOU_GENERATED
```

Replace `THE_HASH_YOU_GENERATED` with the hash from step 2

Save the file. Your Pi will now boot with username `pi` and the password you set.

Step 2: Boot and Connect the Raspberry Pi

1. Eject the SD card from your computer
2. Insert the SD card into your Raspberry Pi
3. Connect the Raspberry Pi to your router using the ethernet cable
4. Plug in the power supply to boot the Pi
5. **Wait about 5 minutes** for the initial boot and setup to complete. The light will be flashing while it sets up for the first time. This is a good time to go grab something tasty to drink.

The Pi needs time to expand the filesystem and complete first-boot configuration. Don't rush this step.

Step 3: Find Your Raspberry Pi on the Network

You need to find the Pi's IP address to connect to it.

Option 1: Using Hostname (Easiest)

On Linux or Mac, try:

```
ping raspberrypi.local
```

If this works, you'll see responses. Press `Ctrl+C` to stop. The IP address will be shown in the output.

Option 2: Using nmap (If hostname doesn't work)

> *WARNING: nmap is a powerful network scanning tool. Use it responsibly and only on networks you own or have permission to scan. You are NOT allowed to use this on public networks or networks you don't have explicit permission to scan. Unauthorized scanning can be illegal and may lead to consequences.*

If `raspberrypi.local` doesn't resolve, use nmap to scan your network:

Install nmap:

- Linux: `sudo apt install nmap`
- Mac/Windows: Download from https://nmap.org/download.html

Find your network range:

```
ip a
```

Look for your active network connection (usually starts with `192.168.x.x` or `10.0.x.x`). Note the subnet. For example, if your computer's IP is `192.168.50.100`, your subnet is likely `192.168.50.0/24`.

Scan for the Raspberry Pi:

```
sudo nmap -sn 192.168.50.0/24
```

Replace `192.168.50.0/24` with your actual subnet.

Look for a result like:

```
Nmap scan report for raspberrypi (192.168.50.227)
Host is up (0.00050s latency).
```

Write down the IP address. You'll need it for SSH and router configuration. In this example, it's `192.168.50.227`.

Step 4: Connect via SSH

Open a terminal and connect to your Pi:

```
ssh pi@192.168.50.227
```

Replace `192.168.50.227` with your Pi's actual IP address.

When prompted:

- Type `yes` to accept the fingerprint (first connection only)
- Enter the password you set earlier

You should now be logged into your Raspberry Pi's command line.

Step 5: Update the Raspberry Pi

Before installing anything, update the system:

```
sudo apt update && sudo apt upgrade -y
```

This may take several minutes depending on how many packages need updating. Let it complete.

Step 6: Install Pi-hole

Pi-hole provides a one-step automated installer. Get the latest command from their GitHub page: https://github.com/pi-hole/pi-hole/#one-step-automated-install

Use their `curl` command shown in github.

Note: Always verify this command on Pi-hole's official GitHub before running it. Install scripts should always be checked against official sources.

During Installation

The installer will guide you through setup:

1. Press Enter to begin
2. Choose your network interface (select the ethernet interface)
3. Select your upstream DNS provider (Cloudflare, Google, OpenDNS, etc.)
4. Use recommended blocklists (yes)
5. Install the web admin interface (yes)
6. Install lighttpd web server (yes)
7. Enable query logging (your choice—yes for visibility, no for privacy)
8. Set privacy mode (choose your preference)

Important: At the end, the installer will display:

- The web interface address (e.g., http://192.168.50.227/admin or http://pi.hole:80/admin)
- Your admin password

Write down the admin password. You'll need it to access the web interface. This is different than your raspbery pi password. Make sure to keep both passwords safe and secure.

If you miss it, you can reset the password later with:

```
pihole -a -p
```

Step 7: Configure Your Router

Now configure your router to use Pi-hole as the DNS server for all devices.

Access Router Settings

1. Open a web browser
2. Navigate to your router's admin panel (commonly `192.168.1.1`, `192.168.0.1`, or `10.0.0.1`)
3. Log in with your router's admin credentials
4. Make sure to update your router's firmware if it has been a while since you've last checked it. This is important for security and performance.

Update DNS Settings

The exact location varies by router, but look for:

- DHCP settings
- LAN settings
- DNS settings
- Network settings

You need to find where DNS servers are configured.

Set both DNS servers to your Pi-hole's IP address:

- Primary DNS: `192.168.50.227` (your Pi's IP)
- Secondary DNS: `192.168.50.227` (same IP)

Why set both to the same address? If you put a different secondary DNS (like Google's 8.8.8.8), devices will use it when Pi-hole is slow or unreachable, bypassing your blocking. Setting both to Pi-hole ensures all DNS traffic goes through it.

Save and Reboot

1. Save the DNS settings

2. Reboot your router if prompted
3. Devices may need to reconnect to wifi or renew their DHCP leases

To force immediate updates, you can:

- Disconnect and reconnect to wifi on each device
- Reboot devices
- Wait for DHCP leases to naturally renew (usually 24 hours)

Step 8: Verify It's Working

Check the Web Interface

1. Open a browser
2. Go to `http://YOUR_PI_IP_ADDRESS/admin` or http://pi.hole:80/admin
3. Log in with the password from installation
4. You should see the Pi-hole dashboard with query statistics

Test Blocking

Visit a site known for heavy ads (news sites work well). Ads should be blocked. Check the Pi-hole dashboard to see blocked queries increasing.

Check DNS on Your Devices

On a device, check its DNS settings:

- It should show your Pi-hole's IP as the DNS server
- If it shows your router's IP, that's fine—the router forwards to Pi-hole

Maintenance

Pi-hole requires minimal maintenance, but stay on top of updates.

Update Pi-hole Monthly

About once a month, SSH into your Pi and run:

```
pihole -up
```

This updates Pi-hole software and blocklists.

Update Raspberry Pi OS

Periodically update the underlying OS:

```
sudo apt update && sudo apt upgrade -y
```

Monitor Performance

Check the web dashboard occasionally to ensure:

- Queries are being processed
- Blocklists are up to date
- The Pi isn't overloaded (unlikely on home networks)

Troubleshooting

DNS not working after setup:

- Verify router DNS settings are saved
- Check that Pi-hole service is running: `pihole status`
- Restart Pi-hole: `pihole restartdns`

Some devices bypass Pi-hole:

- Some devices (smart TVs, IoT gadgets) have hardcoded DNS
- Configure your router to block outbound DNS requests on port 53 except from Pi-hole
- Or use firewall rules to force all DNS through Pi-hole

Sites breaking due to over-blocking:

- Use the web interface to whitelist specific domains
- Adjust blocklist aggressiveness
- Check query logs to see what's being blocked

Pi-hole becomes unreachable:

- Ensure the Pi has a static IP or DHCP reservation
- Check network cables and power
- Access the Pi physically if SSH fails

Next Steps

Now that Pi-hole is running:

- Add additional blocklists through the web interface
- Configure whitelists for sites that break
- Review query logs to understand what your devices contact

Additional Resources

- Official Pi-hole documentation: https://docs.pi-hole.net/
- Pi-hole community forum: https://discourse.pi-hole.net/
- Recommended blocklists: Search "pi-hole blocklists" for curated collections
- Advanced configuration: Look into Pi-hole's gravity database and custom DNS records

Resources for block lists

These are some of the most popular and effective block lists for Pi-hole. You can add them through the web interface under "Group Management" > "Adlists". Always review block lists before adding them to ensure they align with your blocking goals. They will massively increase the number of blocked domains, which can improve privacy but may also cause some sites to break. Start with a few and test your browsing experience before adding more.

- https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
- https://big.oisd.nl/
- Apple Tracker: https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.apple.txt
- https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/adblock/pro.txt
- Gambling: https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/adblock/gambling.txt
- LG: https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.lgwebos.txt
- TikTok Fingerprint Block: https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.tiktok.extended.txt
- Samsung List 1: https://raw.githubusercontent.com/RPiList/specials/refs/heads/master/Blocklisten/samsung
- Samsung List 2: https://gist.githubusercontent.com/wassname/b594c63222f9e4c83ea23c818440901b/raw/1b0afd2aecf3a099f1681b1cf18fc0e6e2fa116a/Samsung%2520Smart-TV%2520Blocklist%2520Adlist%2520(for%2520PiHole)
- Samsung List 3: https://raw.githubusercontent.com/hagezi/dns-blocklists/refs/heads/main/domains/native.samsung.txt

---

Network-level blocking takes effort to set up, but once running, it protects every device automatically.

Pi-hole: Network-Wide Ad and Tracker Blocking for Your Home

February 17, 2026

Browser extensions block ads on your computer. Pi-hole blocks them for every device on your network—phones, tablets, smart TVs, IoT devices—all at once.

What Pi-hole Does

Pi-hole is a DNS-level ad blocker that runs on your local network. It sits between your devices and the internet, filtering DNS requests.

How it works:

- Your devices ask "where is ads.google.com?"
- Pi-hole checks its blocklist
- If the domain is on the list, Pi-hole returns nothing
- The ad or tracker never loads

This happens before data reaches your device, blocking ads and trackers at the network level instead of the browser level.

Why This Matters

Protects devices that can't run ad blockers - Smart TVs, streaming devices, game consoles, and IoT gadgets all make tracking requests. Pi-hole blocks them without requiring software on each device.

Blocks analytics in apps - Mobile apps send telemetry and analytics data constantly. Pi-hole intercepts these requests across all apps on all devices simultaneously.

One configuration for everything - Instead of configuring ad blockers on every phone, tablet, and computer, you configure Pi-hole once and every device benefits.

See what your devices are doing - Pi-hole's dashboard shows every DNS query on your network. You'll see which devices contact which domains, revealing tracking you didn't know was happening.

Faster browsing - Blocked content never downloads, saving bandwidth and speeding up page loads across your entire network.

What Pi-hole Doesn't Block

First-party tracking - If a site serves ads from its own domain (like YouTube), Pi-hole can't distinguish them from regular content.

Embedded content - Ads served from the same domain as the content you want won't be blocked without breaking the site.

HTTPS content inspection - Pi-hole works at the DNS level. It can't see inside encrypted traffic to block specific page elements.

Social media tracking pixels - Some tracking loads from domains that serve legitimate content, making them hard to block without side effects.

Pi-hole complements browser-based blockers, it doesn't replace them. Use both for best results.

Hardware Requirements

Pi-hole runs on minimal hardware:

- Raspberry Pi (any model works, Pi Zero is sufficient)
- MicroSD card
- Power supply
- Ethernet connection (wifi works but ethernet is more reliable)

You can also run Pi-hole on:

- Existing Linux servers
- Virtual machines
- Docker containers
- Old laptops or desktops

It requires very little processing power or memory. If you have spare hardware lying around, it's probably adequate.

Network Impact

Once installed, Pi-hole becomes your network's DNS server. All devices send DNS queries through it. This means:

- Pi-hole is a single point of failure (if it goes down, DNS stops working)
- You need to keep it running 24/7 for continuous protection
- Network performance depends on Pi-hole responding quickly

Most home networks won't notice any slowdown. Pi-hole responses are typically faster than public DNS servers because common domains are cached locally.

Router Firmware Reminder

While setting up network-level blocking, **check your router's firmware**. Outdated router firmware is a security risk:

- Known vulnerabilities stay unpatched
- New exploits can compromise your entire network
- Attackers target routers because they're rarely updated

Make it a habit to check for router firmware updates every few months. Most routers have update options in their admin panel. If your router hasn't been updated in years and the manufacturer no longer supports it, consider replacing it.

Network security isn't just about blocking ads—it's about maintaining the infrastructure that protects your home network.

Privacy Considerations

Pi-hole sees every DNS request from every device. This gives you visibility but also means:

- You're running your own DNS server (with responsibility for maintaining it)
- DNS queries are logged locally by default (you can disable this)
- Anyone with access to Pi-hole's admin panel sees network activity

Configure Pi-hole's privacy settings based on your needs. You can disable query logging entirely if you don't want that data stored.

Next Steps

Before installing:

- Read Pi-hole's official documentation at pi-hole.net
- Decide what hardware you'll use
- Check your router's current firmware version
- Understand that you'll be changing your network's DNS configuration

Pi-hole is powerful for network-wide tracking protection, but it requires basic networking knowledge and ongoing maintenance.

Do Your Research

Before committing to Pi-hole:

- Read reviews from users with similar network setups
- Check which blocklists are most effective for your needs
- Understand the difference between DNS blocking and other ad-blocking methods
- Look into alternative solutions (AdGuard Home, NextDNS) and compare features

Pi-hole is open-source and well-documented. Take time to understand how it works before installing it on your network.

Want to Install It Now?

Check out our tutorial here

Network-level blocking protects devices that can't protect themselves. It's worth the setup effort.

Automated License Plate Readers: What They Track and How to Limit Your Exposure

February 13, 2026

Cameras are tracking your car movements throughout cities, building a database of where you go and when. This isn't speculation, it's infrastructure already deployed across thousands of locations. Here's what you need to know.

What ALPRs Actually Do

Automated License Plate Readers (ALPRs) are AI-powered cameras mounted on poles, buildings, and police vehicles. They photograph every passing vehicle and extract data:

- License plate number
- Date, time, and GPS location
- Vehicle make, model, and color
- Identifying features (bumper stickers, dents, roof racks)
- In some systems, images of passengers and pedestrians

This data gets stored in databases accessible to law enforcement, government agencies, and in some cases, private entities. The cameras don't just catch criminals, they record everyone, all the time, without warrants or probable cause.

Who's Collecting This Data

Flock Safety is one of the largest ALPR vendors in the United States. They sell systems to:

- Police departments
- ICE and other federal agencies
- Private businesses
- Homeowners associations
- Gated communities

The cameras feed data into centralized databases that multiple agencies can access. Your morning commute, grocery store trips, and weekend drives are all logged and searchable.

Other vendors exist, but Flock has been particularly aggressive in deployment. According to Deflock.org, an open-source mapping project, over 75,000 ALPR cameras have been documented across the USA, with over 2,500 in the Dallas-Fort Worth area alone.

The Privacy Problem

Mass surveillance without suspicion - These systems don't target suspects. They record everyone, building movement profiles on people who've done nothing wrong.

Indefinite data retention - How long is your location data stored? Policies vary, but data can be kept for months or years. Your historical movements become a searchable database.

Mission creep - Cameras installed to find stolen cars get used for immigration enforcement, tracking protestors, or monitoring people visiting abortion clinics. The infrastructure enables misuse.

Access without oversight - Different agencies share access to ALPR databases. Who's searching for your car? Why? You likely won't know.

No consent, no notification - You aren't told when you're photographed. You can't opt out. The surveillance is passive and constant.

Real-World Consequences

This isn't theoretical. ALPR data has led to:

- **Wrongful arrests** - Misread plates or database errors put innocent people in handcuffs
- **Profiling** - Tracking vehicles in certain neighborhoods to build immigration or gang databases
- **Stalking by officers** - Police have used ALPR systems to track ex-partners or people they're interested in
- **Movement pattern analysis** - Determining who visits mosques, clinics, protests, or political events

The technology is also inaccurate. Character recognition fails, especially with dirty plates, unusual fonts, or poor lighting. False matches happen regularly.

Security Is Broken

ALPRs are surprisingly vulnerable. Many systems:

- Transmit data unencrypted
- Use default passwords
- Have weak network security
- Can be accessed with basic hacking knowledge

Security researchers have demonstrated that ALPR systems can be compromised to view live feeds or download entire databases. If law enforcement can be hacked, so can you. Your movement data could end up in anyone's hands.

What You Can Do

You can't eliminate ALPR tracking entirely, but you can reduce your exposure.

Know Where Cameras Are

Deflock.org is an open-source project mapping ALPR locations. Check their database to see where cameras are concentrated in your area. Routes with fewer cameras exist if you're willing to take them.

This won't show every camera (new ones deploy constantly), but it gives you awareness of surveillance density.

Limit Identifiable Features

ALPRs catalog more than just plates. They log:

- Bumper stickers (political affiliations, interests)
- Roof racks and bike mounts
- Visible damage or modifications
- Anything that makes your car unique

The more distinct your vehicle, the easier it is to track even without reading the plate. A generic sedan is harder to single out than a car covered in identifying markers.

Change Your Patterns

If you're trying to avoid tracking for a specific trip:

- **Vary your routes** - Don't take the same path every time
- **Use different parking** - Park a few blocks away and walk
- **Time shifts** - Traveling at different times breaks pattern analysis

This is inconvenient and doesn't work for daily commutes, but for sensitive destinations (medical appointments, legal consultations, activism), it adds friction to tracking.

Alternative Transportation

ALPRs track vehicles, not people. Options that avoid car surveillance:

- Public transit (though this has its own surveillance)
- Bicycles
- Walking
- Rideshares (shifts tracking to the driver's vehicle, not yours)

Each has privacy trade-offs. Public transit has cameras. Rideshares log your trips. Nothing is invisible, but you're distributing your data trail.

Obscuring Plates

Some people use plate covers, sprays, or modifications to make plates harder to read. **This is illegal in most jurisdictions** and will get you pulled over. Don't do this unless you understand the legal consequences.

Dirty plates naturally degrade ALPR accuracy, but deliberately obscuring registration is asking for trouble.

Political Action

ALPRs have been banned or restricted in 46 cities, including:

- Austin, TX
- Cambridge, MA
- Eugene, OR
- Sedona, AZ

Local ordinances can limit or prohibit ALPR deployment. If this matters to you:

- Attend city council meetings
- Contact local representatives
- Support organizations fighting surveillance infrastructure
- Vote for candidates who prioritize privacy

Change happens locally. Your city council decides whether to contract with Flock Safety.

The Bigger Picture

ALPRs are one piece of a surveillance ecosystem that includes:

- Facial recognition cameras
- Cell phone location tracking
- Credit card transaction logs
- Social media activity
- Smart home devices

Each system alone is manageable. Combined, they create a comprehensive profile of your life. Addressing ALPRs doesn't solve surveillance, but it's one area where local action can make a difference.

Check Your Area

Before assuming you're being tracked:

- Visit Deflock.org and search for your city
- Look for ALPR cameras on your regular routes (they're often marked with vendor logos)
- Check if your city has contracts with Flock Safety or similar vendors (this is public record)
- Research whether your local government has ALPR policies or restrictions

Knowledge is the first step. You can't avoid what you don't know exists.

Do Your Research

Don't take this article as the complete picture:

- Read ACLU's research on ALPR surveillance
- Check EFF's (Electronic Frontier Foundation) work on tracking technology
- Look into your city's specific ALPR policies
- Follow Deflock.org's updates on camera locations

The landscape changes constantly. Stay informed about what's deployed in your area and who has access to the data.

Surveillance infrastructure is built incrementally. Each camera added seems reasonable until the network is everywhere. Pay attention to what's being installed in your community.

VPN

February 10, 2026

Your phone connects to dozens of networks every week. Each one is a potential window into what you're doing online. Here's how a VPN changes that equation.

What a VPN Actually Does

A VPN creates an encrypted tunnel between your device and the VPN server. Everything you do online goes through this tunnel before reaching the internet. This means:

- Your internet provider can't see what sites you visit
- The wifi network you're on can't read your traffic
- Websites see the VPN server's location, not yours

Think of it as a secure pipe for your data instead of sending it out in the open.

Protection on Public Wifi

Coffee shops, airports, hotels—these networks are convenient but risky. Anyone on the same network can potentially snoop on unencrypted traffic.

A VPN encrypts your connection, so even if someone is monitoring the wifi network, they can't read what you're doing. They'll see encrypted data flowing to a VPN server, nothing more.

This applies to your home wifi too. Your internet provider can see every unencrypted site you visit. A VPN blocks that visibility.

The Cell Tower Threat

Cell tower spoofing (IMSI catchers or "Stingray" devices) is a real concern. These fake towers trick your phone into connecting, then intercept your communications.

What a VPN protects: Your internet traffic. If someone spoofs a tower and monitors your data connection, they'll only see encrypted VPN traffic. They won't know what sites you're visiting or what you're doing online.

What a VPN doesn't protect: Your calls, texts, and location data. Those go through the cellular network separately and aren't protected by a VPN. The fake tower still knows your phone is nearby.

VPNs help with internet privacy, not cellular communication privacy. Know the difference.

Bypassing Geographic Restrictions

Some countries, workplaces, or networks block certain websites. Others restrict content based on your location.

A VPN changes your apparent location. When you connect to a server in a different country, websites think you're accessing from that location. This can help you:

- Access sites blocked in your region
- Bypass workplace or school network restrictions
- View content that's geo-restricted

If you're traveling to or living in a place with heavy internet censorship, a VPN is one tool to maintain access to the open internet. Research which VPN protocols work best in restricted regions—some governments actively block VPN traffic.

Breaking Up Your Data Trail

Advertisers, data brokers, and trackers build profiles by connecting your activity across different sites. Your IP address is one piece they use to link everything together.

Randomizing your VPN server daily makes tracking harder. Each day you appear to be browsing from a different location with a different IP address. This fragments your digital footprint.

Does this make you anonymous? No. You're still logged into accounts, using the same browser fingerprint, and carrying device identifiers. But it adds friction to the tracking process. Data brokers need to work harder to connect the dots.

Think of it as one layer in a broader privacy strategy, not a magic solution.

Mobile-Specific Benefits

Your phone is always connecting—updating apps, syncing data, checking email. Much of this happens in the background on whatever network you're connected to.

A VPN on your phone means:

- All those background connections are encrypted
- Your location isn't broadcast through your IP when you quickly check something
- You're protected the moment you connect to any network, automatically

Some VPNs have a kill switch feature on mobile. If the VPN connection drops, it blocks internet access until the VPN reconnects. This prevents accidental unencrypted exposure.

What a VPN Can't Do

Be clear about the limitations:

- **It doesn't make you anonymous**. Your accounts still identify you.
- **It doesn't stop app tracking**. Apps can fingerprint your device through other means.
- **It doesn't protect against malware or phishing**. Those are separate security concerns.
- **It might slow your connection**. Encryption and routing through remote servers adds overhead.
- **It requires trust**. Your VPN provider sees what your ISP used to see. Choose carefully.

Make It a Habit

Privacy isn't a switch you flip once. It's a practice:

- Turn on your VPN before connecting to public wifi
- Randomize servers periodically to fragment your trail
- Use it when accessing sensitive information on the go
- Combine it with other privacy tools (encrypted messaging, privacy-focused browsers)
-

What We Use

I use Proton, just because its easy and fairly cheap. They claim a no-logs policy and operates under Swiss privacy laws, but verify this yourself through independent audits and reviews. Since Proton also has a suite of other tools, it can integrate nicely with the rest of their ecosystem. Same account, same privacy principles, open-source code. If you're already using Proton Mail, it's an easy extension.

The free tier exists but is limited. Paid plans offer faster speeds, more servers, and advanced features. Like Proton Mail, you're paying for the service instead of being the product.

Do Your Research

Don't rely solely on this article. Look into:

- Independent VPN audits and tests
- How VPNs actually work at the technical level
- What data Proton VPN collects (check their privacy policy)
- Whether your threat model actually requires a VPN

Understanding the tool makes you better at using it. A VPN is powerful for mobile privacy, but only if you know what it does—and what it doesn't.

A VPN is one piece of a privacy strategy, not a complete solution. Use it intentionally.

Removing Google From Your Website: Fonts, Analytics, and Maps

May 14, 2026

Every time someone visits your site with Google Fonts, Google Analytics, or Google Maps embedded, you're sending their data to Google. IP addresses, browser fingerprints, and behavior patterns—all collected without meaningful consent. Here's how to stop that.

Why This Matters

Google offers free services for a reason: data collection. When you embed Google's code on your website:

Google Fonts - Google logs every visitor's IP address, browser type, and which pages load which fonts. They build profiles across millions of websites.

Google Analytics - Tracks user behavior, page views, session duration, and clicks. Google ties this to their advertising network to target users across the web.

Google Maps - Collects location data, search queries, and browsing patterns. Every embedded map is a tracking beacon.

You might not care about this data, but your visitors probably do. You're making privacy decisions on their behalf by choosing these tools.

Self-Hosting Google Fonts

Google Fonts are just font files. There's no technical reason to load them from Google's servers. Self-hosting is straightforward and faster.

Why Self-Host

- No requests to Google servers (Google can't log your visitors)
- Faster page loads (one less external connection)
- Works without internet access to Google's CDN
- No GDPR concerns about third-party data processing
- Complete control over font delivery

How to Self-Host Fonts

Step 1: Download the font files

Download directly from Google Fonts and extract the font files you need (usually `.woff2` for modern browsers).

Step 2: Add fonts to your project

Create a `fonts` directory in your website's assets:

```
/assets
  /fonts
    roboto-regular.woff2
    roboto-bold.woff2
```

Step 3: Update your CSS

Replace the Google Fonts `<link>` tag in your HTML with a local `@font-face` declaration in your CSS:

Old method (loads from Google):

```
<link href="https://fonts.googleapis.com/css2?family=Roboto:wght@400;700&display=swap" rel="stylesheet">
```

New method (self-hosted):

```
@font-face {
  font-family: 'Roboto';
  font-style: normal;
  font-weight: 400;
  font-display: swap;
```

```
  src: url('/assets/fonts/roboto-regular.woff2') format('woff2');
}

@font-face {
  font-family: 'Roboto';
  font-style: normal;
  font-weight: 700;
  font-display: swap;
  src: url('/assets/fonts/roboto-bold.woff2') format('woff2');
}

body {
  font-family: 'Roboto', sans-serif;
}
```

That's it. Your fonts now load from your server. No Google tracking.

Performance Tip

Use `font-display: swap` to prevent invisible text during font loading. The browser shows fallback fonts immediately, then swaps to your custom font when loaded.

Only include font weights you actually use. Every weight is a separate file. If you only use regular and bold, don't include light, medium, or black weights.

Replacing Google Analytics

Analytics tools track visitors to help you understand traffic patterns. But most websites don't need this level of data—and definitely don't need to send it to Google.

Do You Even Need Analytics?

Ask yourself:

- What decisions do you make based on analytics data?
- Would your site function without knowing visitor counts?
- Do you actually check your analytics regularly?

For personal blogs, portfolios, and small business sites, **the answer is often no**. You're collecting data out of habit, not necessity.

Alternative: Direct User Feedback

Instead of tracking page views, ask visitors what they want:

- Add a feedback form or email address
- Include "Was this helpful?" buttons on content
- Monitor what people contact you about
- Pay attention to which pages get linked or shared

Direct feedback tells you what matters to users. Analytics tells you what they clicked. The former is more valuable and doesn't require surveillance.

Privacy-Respecting Analytics Alternatives

If you genuinely need analytics, use tools that respect user privacy. Use your favorite search engine and search for "privacy focused web analytics" and you'll find a ton of results. These services collect basic metrics (page views, referrers, device types) without building user profiles or selling data to advertisers.

Self-Hosting Analytics

If you're technical, self-host analytics on your own server. Self-hosting means data never leaves your infrastructure. You control retention, access, and privacy policies completely.

Replacing Google Maps

Google Maps is convenient but sends location data, search queries, and IP addresses back to Google every time someone interacts with your embedded map.

OpenStreetMap as the Base

OpenStreetMap (OSM) is a community-built mapping database. It's open data that anyone can use without tracking users.

You don't embed OSM directly, you use a library that renders OSM tiles. The most popular is **Leaflet**.

Using Leaflet for Maps

Leaflet (https://leafletjs.com) is a lightweight JavaScript library for interactive maps using OpenStreetMap data.

Basic implementation:

1. Include Leaflet CSS and JS in your HTML:

```
<link rel="stylesheet" href="https://unpkg.com/leaflet@1.9.4/dist/leaflet.css" />
<script src="https://unpkg.com/leaflet@1.9.4/dist/leaflet.js"></script>
```

2. Add a map container:

```
<div id="map" style="height: 400px;"></div>
```

3. Initialize the map with JavaScript:

```
// Create map centered on specific coordinates
const map = L.map('map').setView([51.505, -0.09], 13);

// Add OpenStreetMap tiles
L.tileLayer('https://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png', {
  attribution: '© OpenStreetMap contributors'
}).addTo(map);

// Add a marker
L.marker([51.505, -0.09]).addTo(map)
  .bindPopup('Your location here')
  .openPopup();
```

That's a functional map with no Google tracking.

Tile Servers

OpenStreetMap tiles are free but shouldn't be used for high-traffic commercial sites (their servers can't handle the load). Options:

- **MapTiler** - Paid tile hosting with free tier
- **Mapbox** - Commercial tile provider with generous free tier
- **Self-host tiles** - Run your own tile server (complex but fully private)

For small sites, OpenStreetMap's default tiles work fine. For larger sites, use a commercial tile provider or self-host.

Leaflet Alternatives

- **Mapbox GL JS** - More features, heavier library
- **OpenLayers** - Powerful but more complex
- **MapLibre GL** - Open-source fork of Mapbox GL

Leaflet is the easiest starting point for most use cases.

The GDPR Angle

If you serve European users, GDPR requires consent for non-essential tracking. Google Analytics, Fonts, and Maps all trigger consent requirements because they send data to third parties.

By removing Google services:

- You eliminate most third-party tracking
- You reduce or eliminate cookie banner requirements
- You simplify compliance

Privacy-respecting alternatives often don't require consent banners because they don't track users across sites or build profiles.

Check your local regulations, but removing Google tracking typically simplifies legal compliance significantly.

Performance Benefits

Removing Google services often makes your site faster:

Fonts - One less DNS lookup, one less HTTPS connection, fonts cached on your domain **Analytics** - No external script blocking page rendering **Maps** - Leaflet is lighter than Google Maps API

Fewer third-party requests means faster page loads and better user experience.

Implementation Checklist

To remove Google from your website:

- [ ] Download font files and update CSS with `@font-face`
- [ ] Remove Google Analytics script tag
- [ ] Choose analytics alternative (or skip analytics entirely)
- [ ] Replace Google Maps embeds with Leaflet + OpenStreetMap
- [ ] Update privacy policy to reflect changes
- [ ] Test all pages to ensure fonts and maps work
- [ ] Monitor for broken functionality

Your website visitors didn't consent to be tracked by Google. Stop making that decision for them.