A FREE GUIDE FROM KAMSIOB

Block Ads & Trackers on Everything You Own, for Free

Most apps quietly report your behavior to ad and analytics companies, and most “free” blockers want a subscription or your data. This guide sets up system-wide ad and tracker blocking that works on every network, using two genuinely free services, in about twenty minutes. Set it once and forget it. No tech background needed.

- own it, don't rent it
- keep it private
- keep it simple

WHAT IT COSTS

- **NextDNS** free tier (blocks ads & trackers on every network)
- **Tailscale** free for personal use (connects it all together)
- **Total** **$0.** No trials, no cards, no catch. Both companies make their money on business plans, not on you

WHAT THIS DOES

- ✓ Blocks most ads and app trackers on every network, automatically
- ✓ Breaks most cross-app tracking profiles
- ✓ Works identically at home, on mobile data, on public Wi-Fi
- ✓ Costs nothing and runs itself once set up

WHAT IT HONESTLY DOESN'T

- ✗ Make you anonymous to sites you log into (Google still knows what you do on Google)
- ✗ Block every single ad (a few, like YouTube's, come from the same place as the content)
- ✗ Change anything for other people in your household. This affects only your own devices

BEFORE YOU START

You'll need an Android phone, a browser, and about twenty minutes. Follow the parts in order. Each one ends with a way to check it worked before you move on. Everything here is ordinary, fully legal consumer software used exactly as it's sold.

PART 1 NextDNS

your ad & tracker blocker. one account, set once.

1. In a browser, go to `my.nextdns.io` and sign up. It's free and only needs an email.
2. After signing up, look near the top of the page for a **six-character ID** (something like `abc123`). Screenshot it or write it down. You'll need it in Part 3.
3. Click the **Privacy** tab. Click **Add a blocklist**, search for **HaGeZi Multi Pro**, and add it. This is the list of ad and tracker addresses that will get blocked.
4. In the same Privacy tab, make sure **Block Disguised Third-Party Trackers** is turned ON.
5. Ignore NextDNS's own setup instructions completely. There is no app to install. You're done here.

> **GOOD TO KNOW**
> The free tier covers 300,000 lookups a month, which is plenty for one person. If you ever pass it, blocking pauses until the next month. Nothing breaks.

PART 2 Tailscale

connects your devices privately and carries the blocking everywhere.

6. On your Android phone: install **Tailscale** from the Play Store, open it, and sign up. You can log in with a Google, Microsoft, or GitHub account.
7. Optional but recommended: install Tailscale on your computer too, from `tailscale.com/download`, and log into the **same account**. This lets your phone reach your computer securely from anywhere, which becomes useful for syncing files and notes later.

> **CHECK IT WORKED**
> Open the Tailscale app on your phone. Every device you signed in on should appear in the device list.

PART 3 Connect them

the one-time link that makes blocking automatic on every network.

8. In a browser, go to `login.tailscale.com/admin/dns` and log in with the same account.
9. Under **Nameservers**, click **Add nameserver** and choose **NextDNS** from the list.
10. Paste the six-character ID you saved in Part 1, step 2. Save.
11. On the same page, turn ON **Override DNS servers**. This is the important switch: it makes every device on your account actually use the blocking, on any Wi-Fi and on mobile data.

> **CHECK IT WORKED**
> On your phone, with Tailscale connected, visit `test.nextdns.io` in your browser. It should say status **ok** and show your ID. If it does, ad and tracker blocking is now live on all your devices, everywhere. Most of the value of this whole guide is already working right here.

PART 4 Lock it in

make it permanent so it survives reboots and never leaks.

12. On your phone: **Settings > Network & internet > VPN**, tap the gear next to Tailscale, then turn ON **Always-on VPN** and **Block connections without VPN**.
13. If you were using another ad-blocking app that works as a VPN (AdGuard, Blokada, RethinkDNS and similar), uninstall it now. Android only allows one app in that role, and its job is covered by what you just built.

> **GOOD TO KNOW**
> Also worth doing while you're in Settings: **Privacy > Ads > Delete advertising ID**. This breaks the ID that apps use to link your activity together into one profile.

HOW YOU'LL LIVE WITH THIS DAY TO DAY

Nothing. That's the point. Blocking is always on and invisible, on every network, and there are no toggles to manage and no apps to open. If a website ever breaks, log into `my.nextdns.io`, open the Logs tab, find the blocked domain, and allow it.

WANT TO GO FURTHER?

This setup blocks trackers, but your internet and cell provider can still see which sites you visit (and in the US, they sell that). Closing that last gap takes a real VPN, and there's a companion Kamsiob guide that adds one to this exact setup for a flat $5/month. Same steps you just did, plus one more part.

Thanks for reading. Genuinely. – Kam

youtube.com/@kamsiob github.com/kamsiob kamsiob.com hello@kamsiob.com

this guide is free to share. it collects nothing about you. it wouldn't be very me otherwise.