

THE 90-MINUTE PRIVACY EMERGENCY KIT

Three Leaks. Three Fixes. A Real Head Start.

A free resource from

LEAVE ME ALONE

Take Back Your Privacy Without Disappearing

by Archer Vance

Before You Start

This is adapted from the opening 90-minute walkthrough in *Leave Me Alone* — given to you free because it stands on its own. If it helps, the full book covers everything this kit doesn't: your car, your smart home, your health apps, your accounts at work, and the data that's already out there, not just the leaks going forward.

No email required to have this. If you'd like updates when new tools or opt-out procedures change, there's an optional signup at the end — entirely up to you.

Three Leaks. Three Fixes. A Real Head Start.

These three leaks are destroying your privacy right now. Here's how to plug them before dinner.

You just saw what's exposed. Google results. Data broker profiles. Your face indexed across the internet.

Now you want to fix it. But here's the problem: you're looking at hundreds of hours of work. Delete this account, opt out of that broker, adjust fifty privacy settings, learn new tools, change old habits.

It's overwhelming. Which is exactly why most people do nothing.

So we're not starting there. We're starting with three of the most consequential structural privacy leaks — weaknesses that, once patched, immediately and measurably reduce your exposure.

Fix these three things, and you'll:

- Break the links between your scattered online identities
- Stop your personal information from being sold in bulk
- Prevent future data accumulation before it starts
- Cut your trackable footprint meaningfully — without a hundred hours of work

Total time: 90 minutes · Total cost: \$0–15 · Difficulty: Easy enough to do while watching TV

This isn't the complete solution. But it's the foundation everything else builds on. Think of it like triaging a patient in the emergency room — you don't start with the bruises. You stop the bleeding first.

Three leaks. Three fixes. Ninety minutes. Let's go.

△ PROGRESS TRACKER

- ☐ Leak #1: Email compartmentalization (30 min)
- ☐ Leak #2: Phone number protection (30 min)
- ☐ Leak #3: Social media lockdown (30 min)
- ☐ Completion: Run quick verification test

Leak #1: Your Email Address = Master Key to Your Life

Time required: 30 minutes · Cost: \$0 (free tier) or \$12/year (premium)

The Problem: One Email Connects Everything

You probably use one or two email addresses for everything. That single email is the thread that ties your entire digital life together.

When data brokers, advertisers, and analytics platforms want to connect your activities across dozens of websites, they use your email as the matching key — hashing it and matching that hash against billions of other hashed emails in their databases. Every account, every purchase, every login is now linked to one person: you.

The Fix: Email Compartmentalization

The solution isn't to abandon email. It's to break the connection between your scattered accounts by using different emails for different purposes — the 4-email system:

- #1 Primary Identity — banking, government, taxes, healthcare, legal, insurance. Maximum security. Never used for shopping or social media.
- #2 Social & Personal — friends, family, professional networking.
- #3 Shopping & Services — online shopping, subscriptions, bookings. Use an aliasing service so every merchant gets a unique address.
- #4 Throwaway & Testing — one-time signups, sketchy sites. Fully disposable.

Step-by-Step Setup (30 Minutes)

Task 1: Set up email aliasing (15 min) — SimpleLogin (simplelogin.io) is a solid free option (roughly 10 free aliases as of this writing — verify current limits on their pricing page, as free-tier terms shift). Sign up with your Email #2, create a unique alias per merchant, and forward to Email #3. If spam arrives at an alias, you know exactly who sold it — disable that alias without affecting anything else. Addy.io, Firefox Relay, and Apple Hide My Email are solid alternatives.

Task 2: Check Have I Been Pwned (5 min) — Go to haveibeenpwned.com and enter your primary emails. If you've been “pwned,” change those passwords immediately, enable app-based 2FA, and treat those emails as burned for high-security uses. Set up ongoing alerts at haveibeenpwned.com/NotifyMe.

Task 3: Create a compartmentalization plan (10 min) — List your accounts (check your password manager; search your inbox for “welcome,” “verify,” “confirm”), and assign each to the right tier. Migrate high-priority accounts (banking, healthcare) this week, medium-priority (shopping, social) this month, and use aliases for everything new going forward.

Expected Result

After 30 minutes: email aliasing is live, breach monitoring is active, and you have a migration plan. Within 30 days, as you migrate accounts, your most sensitive data is no longer linked to shopping or social activity, and cross-platform tracking via email matching is broken.

This is one of the highest-impact changes you can begin in 90 minutes — it's the fix everything else in the book builds on.

Leak #2: Your Phone Number = Permanent Tracking Beacon

Time required: 30 minutes · Cost: \$0 (Google Voice) or \$3–10/month (MySudo, Hushed)

The Problem: It Never Changes, and Everyone Has It

Unlike email, your phone number tends to stick with you for decades — and everyone wants it: social media, banks, retailers, doctors, apps, landlords. It becomes a permanent identifier.

Carriers log every cell-tower ping and sell that location data to brokers, marketers, and law enforcement. Companies like Telesign and Neustar assign your number a “reputation score.” Scammers buy Do Not Call registries precisely because they’re lists of verified, active numbers.

The Fix: The 3-Number Strategy

- #1 Real Personal Number — family, close friends, emergency contacts, healthcare only. Treat it like a Social Security number.
- #2 Semi-Public (Burner) — deliveries, services, online accounts. Google Voice (free), MySudo, or Hushed. Disposable if spammed.
- #3 Throwaway (Temp) — one-time verifications only. Fully recycled, never for anything important.

Step-by-Step Setup (30 Minutes)

Task 1: Set up Google Voice (15 min) — Go to voice.google.com (ideally with a separate Google account), choose a new number, and link it to your real phone for forwarding. Give this number out instead of your real one going forward. Google Voice numbers can be changed, but historically only about once a year and sometimes for a small fee — check current terms at voice.google.com before counting on swapping it freely.

Task 2: Identify accounts with your real number (10 min) — Check your password manager and search your inbox for “phone,” “verification,” “SMS.” Prioritize: keep your real number only for banking, healthcare, government, and emergency contacts.

Task 3: Begin migration — Use Google Voice for all new signups immediately. Migrate medium-priority accounts over the next month. Switch phone-based 2FA to an authenticator app wherever offered — SIM-swapping and SMS interception make phone-based 2FA a real vulnerability. Google Authenticator, Microsoft Authenticator, Aegis (Android), and 2FAS are solid current choices; Authy’s desktop app has been discontinued and its long-term support is uncertain, so it’s no longer a top pick.

Expected Result

After 30 minutes: your burner number is active and you have a migration plan. Within 30 days, your real number is shared with a much smaller, deliberately chosen group, your burner absorbs the spam, and you’re no longer dependent on your phone number for account security.

Combined with Leak #1, this closes off two identifiers commonly used to link activity across services.

Leak #3: Social Media = Public Data Goldmine

Time required: 30 minutes · Cost: \$0

The Problem: You've Posted Your Life Story

Every photo, check-in, like, friend connection, and comment can add to the information platforms collect and use to personalize your experience and advertising. Information you make public can also be viewed, copied, or scraped by outside parties — including people and automated systems you never intended to share it with.

The Fix: Platform-by-Platform Lockdown

A note before you start: verified against current platform documentation as of this writing, but social platforms redesign settings menus often. If a path below doesn't match what you see, search “[platform] privacy settings” for the current location — the goal described is what matters. This is exactly the kind of thing the book's companion updates page is meant to keep current.

Facebook (10 min): Download your data archive first (profile icon → Settings & Privacy → Settings → Accounts Center → Your Information and Permissions → Download Your Information) to see everything they have. Then, also in Accounts Center: hide your friends list, disable search-engine linking, turn off location history, disable facial recognition, remove all third-party apps, and disconnect what Meta now calls “Your Activity off Meta Technologies” (formerly Off-Facebook Activity).

Instagram (7 min): Switch to a private account, turn off story sharing and contact syncing, review connected accounts in Accounts Center and disconnect any you don't need linked, and disable location services.

Twitter/X (7 min): Protect your posts, turn off email/phone discoverability, disable location tagging, and turn off personalized ads.

LinkedIn (6 min): Use private profile-viewing mode, limit what non-connections see, and restrict messaging to connections only.

Expected Result

After 30 minutes: your major platforms are locked down, off-platform tracking is reduced, and your public attack surface for scammers and stalkers is smaller — while any professional presence you need stays intact.

This is the most visible fix of the three — friends and family won't notice, but you'll expose less information publicly for automated collection and casual lookup.

Emergency Kit Complete

You just closed three major structural leaks in 90 minutes. That's not the complete solution — but it's a real, defensible head start, and the foundation everything else in the book builds on.

What This Doesn't Do

These fixes stop new data from leaking. They prevent future tracking. They break ongoing connections. What they don't do is delete the data that already exists — your data broker profiles, your search results, your face in facial recognition databases, years of accumulated digital exhaust.

That's what the rest of *Leave Me Alone* covers: the 30-day roadmap to actually delete what's already out there, plus dedicated chapters on your email and phone at a deeper level, your browser, your social accounts, your smart home, your car, your job, your finances, your health data, and your travel — the parts of your life a 90-minute kit was never going to reach.

Want the rest?

Leave Me Alone: Take Back Your Privacy Without Disappearing is available on Amazon in ebook and paperback.

For updates, corrected procedures as companies change their settings, and additional resources tied to this book — entirely optional, never required — visit leavemealoneprivacy.com. Your email isn't the price of admission.

Archer Vance has no social media presence, no public email address, and no speaking circuit. This resource is the extent of the contact.