THE PRIVACY EXPOSURE AUDIT

A 30-Question Self-Assessment

2025-2026 EDITION

by TRUCE

TABLE OF CONTENTS

INTRODUCTION

Most people don't know how exposed they are until something bad happens. A SIM swap drains the account. A stalker shows up. A doxxing campaign starts. Their location data appears in a context they didn't expect. By then, they're playing defense.

This audit puts a number on your current exposure. Thirty questions. Answer honestly. Each "yes" is a point. At the end, you'll know exactly where you stand and what to do about it.

The questions are organized by category. Each one comes with a brief explanation of why it matters and what fixing it looks like. You're not just answering, you're learning what to look for.

This isn't a sales pitch. It's a diagnostic. Some people will finish and realize they're in better shape than they thought. Others will finish and realize they have real work to do. Both outcomes are useful.

How to use this audit

Read each question carefully. Answer yes or no based on your current reality, not what you intend to fix later. Keep a running count of your "yes" answers. At the end, you'll find a scoring guide that tells you what your number means and what to do next.

If you're uncertain about a question, the answer is probably yes.

Let's get started.

SECTION 1: HOME AND PHYSICAL ADDRESS

1. Does your real home address appear when someone searches your full name on Google or a people-search site (BeenVerified, Spokeo, WhitePages, Radaris)?

Data brokers aggregate your address from voter rolls, property records, utility connections, and old marketing lists. If it's on people-search sites, anyone with five dollars can find you. This is the single most common exposure for adults in the U.S.

Fix: aggressive data broker removal as a recurring habit, ideally combined with shifting your "public" address to a private mailbox or registered agent.

2. Did you register to vote at your current home address?

Voter registration is public record in most states. Many people-search sites pull from voter rolls directly. Anyone can search your name and see your registration address.

Fix: state-dependent. Some states allow alternative addresses for voter registration. Others don't. Know your state's rules before deciding the trade.

3. Is your home titled in your personal name (or jointly with a spouse)?

Property records are public. Anyone can search the county assessor's website by your name and find your home. This is one of the highest-impact exposures for high-net-worth individuals because it confirms

ownership, value, and address all in one record.

Fix: hold property in an LLC or land trust. Wyoming, New Mexico, and Delaware are best for anonymous LLC structures.

4. Does your driver's license list your current home address?

Every time you hand over your ID at a bar, airport, hotel, gym, or doctor's office, your home address is exposed. Many states allow you to use an alternate address on your license (a private mailbox or registered agent in some cases).

Fix: file for an address change if your state allows alternate addresses. If not, consider whether moving your legal residence is on the table.

SECTION 2: PHONE AND CELLULAR

5. Did you set up your current cell phone account in your real name with your real home address?

Your carrier has your full identity and a documented history of selling real-time location data. Every tower you connect to is logged.

Fix: LLC business cellular, prepaid in an alias, or data-only eSIM with VoIP for voice and SMS.

6. Do you give your real cell number out to banks, businesses, doctors, retailers, or anyone other than family?

Every account with your real number is a potential SIM swap path and a tracking data point. Your cell number is in dozens of breached databases by now.

Fix: multiple VoIP numbers (VoIP.ms) for different purposes. Real cell only for family.

7. Do any of your important accounts (email, banking, investment, crypto) use SMS for two-factor authentication?

A SIM swap takes one social-engineered carrier rep. Once an attacker has your SMS codes, they reset your email password, then your bank, then drain accounts in under an hour.

Fix: hardware security keys (YubiKey) for the highest-value accounts. Authenticator apps (Aegis is best, avoid Google Authenticator) for everything else.

8. Have you ever set up a port-out PIN or "number lock" with your carrier?

This is one phone call to your carrier and the single highest-leverage SIM swap defense available to a regular customer. Most people skip it.

Fix: call your carrier today and set it up. T-Mobile calls it "NOPORT," Verizon calls it "Number Lock," AT&T; calls it "Wireless Account Lock."

9. Is your phone's cloud backup using default encryption (no Advanced Data Protection on iCloud, no E2EE on Google backup)?

Without end-to-end encryption, your phone's entire backup including messages, photos, and saved passwords is decryptable by Apple or Google. They will hand it over under legal process. They have the keys.

Fix: enable Advanced Data Protection on iPhone (Settings > Apple ID > iCloud > Advanced Data Protection). On Android, move to GrapheneOS with Seedvault for E2EE backup.

SECTION 3: FINANCIAL ACCOUNTS

10. Does your bank, brokerage, or crypto exchange have your real home address on file?

Financial institutions are heavily breached. When (not if) they leak, your home address goes with it. Banks are also legally required to share information with various government and tax agencies.

Fix: many institutions accept a private mailbox as the mailing address while keeping legal residence private. Worth asking.

11. Do you use the same email address for sensitive accounts (banking, brokerage) as you do for shopping, signups, and social media?

Your "main" email is in dozens of breached databases. If it's the same one on your bank, attackers can target you directly with phishing or credential stuffing.

Fix: dedicated sensitive email (Proton or Tuta), aliased shopping email, never crossed.

12. Are your bank or brokerage accounts protected only by SMS 2FA?

Same SIM swap vulnerability as the phone section, except here the consequences are direct theft. Most major banks now support hardware keys or authenticator apps. Most people never switch.

Fix: audit every financial account today. Replace SMS with hardware key or authenticator app.

13. Do you store cryptocurrency on an exchange (Coinbase, Binance, Kraken) instead of a self-custody wallet?

Exchanges are honey pots for SIM swap attackers because crypto converts and moves quickly. They're also subject to seizure, freeze, and exchange insolvency.

Fix: hardware wallet (Ledger or Trezor) with seed phrase stored offline in two physical locations. Keep only what you're actively trading on an exchange.

SECTION 4: IDENTITY AND GOVERNMENT RECORDS

14. Has your name, address, or social security number been in any major data breach you know of?

Spoiler: yes. Equifax, Anthem, T-Mobile, AT&T;, the list is endless. Your past data is already out there.

The question isn't whether you've been breached. It's what new data you're generating going forward, and whether you're treating your historical exposure as a permanent reality you need to defend around.

Fix: assume your past is exposed, focus on what new data you generate from here.

15. Are your utility bills (electricity, water, gas, internet) in your real name at your real address?

Utility records are sold to data brokers. Every utility account feeds your address into the broader data ecosystem and makes you findable.

Fix: utilities in LLC name where landlords/utility companies allow. Some require personal guarantees. Pick your battles.

16. Do you have a public LinkedIn profile that lists your current employer and city?

LinkedIn is the most useful tool for stalkers, social engineers, and BEC scammers in existence. Your employer, location, role, and connection network all in one place.

Fix: minimum information, vague city (e.g., "New York metro area"), no specific employer if you can avoid it. If LinkedIn is necessary for your career, accept the trade and lock down everything else.

SECTION 5: DIGITAL FOOTPRINT

17. Have you opted out from major data broker sites (Spokeo, WhitePages, BeenVerified, Radaris) in the last 12 months?

Data brokers re-aggregate your info constantly. Opt-outs aren't permanent. Quarterly opt-outs are the minimum maintenance.

Fix: services like DeleteMe, Kanary, or EasyOptOuts handle the ongoing work. Or do it yourself quarterly with a documented checklist.

18. Do you use a unique strong password for every account, generated by a password manager?

If you reuse passwords, one breach gives attackers access to everything. Credential stuffing is the most common attack vector against everyday users.

Fix: Bitwarden (open source) or 1Password. Unique generated password per account, master password memorized and not stored anywhere.

19. Do you use a VPN whenever you're on Wi-Fi outside your home (cafes, airports, hotels)?

Public Wi-Fi networks are frequently compromised or actively malicious. Your traffic is exposed to whoever owns the router and anyone watching.

Fix: paid VPN (Mullvad, Proton VPN, or IVPN), always on for public Wi-Fi. Free VPNs sell your data, defeating the purpose.

20. Is your primary Google account or iCloud account associated with your real name and real phone number?

Both Google and Apple have everything about you. Even with privacy settings on, their internal records have your full identity tied to your search history, location history, and communications.

Fix: alias accounts for sensitive activity, separate from your "civilian" identity. Migration to E2EE alternatives (Proton, Tuta) for anything truly sensitive.

SECTION 6: SOCIAL MEDIA AND PUBLIC PRESENCE

21. Do you post photos on social media (Instagram, Facebook, X, TikTok) with location data, recognizable landmarks near your home, or your daily routine?

Stalkers and burglars use social media for reconnaissance. Photo metadata sometimes contains GPS coordinates. Even without metadata, recognizable backgrounds give you away.

Fix: strip metadata before posting, post on delay (not in real time), never tag locations near your home.

22. Does your social media profile show your full real name?

Your name is the master key to everything else. Once someone has it, they can search public records, data brokers, court records, and breached databases.

Fix: alias name on public-facing accounts. Real name only on accounts that legally require it.

23. Do you accept friend or follow requests from people you don't actually know?

Social engineers and stalkers create fake profiles to access friends-only content. Many doxxing attacks start with a fake friend request.

Fix: only accept people you've met in person or have verified relationships with. Periodically audit your followers and remove ones you don't recognize.

24. Have you ever posted a photo of your home's exterior, your street view, or your neighborhood from a recognizable angle?

One photo of your front door is enough for someone to find your address with reverse image search and Google Street View. Same for distinctive neighborhood features.

Fix: never post exterior photos of your home. Ask family to do the same. Take down old posts that show this information.

SECTION 7: VEHICLES

25. Is your vehicle titled in your real name with your real home address on the registration?

Vehicle registration is public record in most states. Anyone with your plate can run it (or pay a service to run it) and find your name and home address.

Fix: title in an LLC, use the registered agent address. Wyoming and Montana have specific frameworks for this.

26. Does your car insurance list your real home address?

Insurance records leak. Plus, your insurance company sells data to marketing aggregators and to companies that build risk profiles on you.

Fix: LLC ownership flows through to insurance. If LLC titling isn't on the table, ask your insurer about alternate mailing addresses.

27. Do you use a toll transponder (E-ZPass, SunPass, FasTrak) tied to your real name and address?

Toll records are subpoena-friendly and have been used in stalking, divorce, and surveillance cases. They map every highway you take, with timestamps.

Fix: LLC-registered transponder, or pay cash for tolls during movements you don't want recorded.

SECTION 8: FAMILY AND NETWORK

28. Do your immediate family members (spouse, kids, parents) appear in public records with addresses linkable to yours?

Even if you're locked down, a search for your spouse's name finds your shared home. Your kids' school records, your parents' obituary mentions, all of it leaks.

Fix: family-wide privacy planning, not just yours. The conversations are uncomfortable but necessary if you're serious about this.

29. Do your friends or family post about you on social media in ways that reveal your location, routine, or relationships?

You can't lock down your privacy if everyone around you is broadcasting. Holiday photos, birthday tags, "girls trip" tags, all of it leaks your location and routine.

Fix: have the conversation with your inner circle. They don't have to live your privacy life, but they need to respect a few rules around your name and your home.

30. Have you ever sent sensitive personal info (address, phone, SSN, financial account numbers) in a text message, email, or DM?

Those messages live forever in the platform's servers, the recipient's device, and probably their cloud backup. One breach away from exposure.

Fix: Signal with disappearing messages for sensitive info. Never SMS or email for anything that could enable identity theft if leaked.

SCORING

Count your total "yes" answers. Maximum score is 30.

Write your number here: _____

WHAT YOUR SCORE MEANS

0 to 7: Already Strong

You've done meaningful privacy work. You're well above average. Focus on maintenance: quarterly audits, staying current on tool recommendations, watching for new exposures as you change addresses, jobs, or platforms.

If you're at this level and still feel exposed, your situation is probably specific (public figure, stalker, professional risk). A consultation can help you triage what's left.

8 to 14: Concerning

You have meaningful gaps. The good news: most of these gaps you can close yourself in a few weekends if you commit. The bad news: gaps compound. One leak fills in another. You're not in crisis but you're not safe either.

Recommended next moves:

- Set a carrier port-out PIN today (15 minutes)
- Move bank, email, and brokerage 2FA off SMS this week (1 hour)
- Download the Phone Privacy Guide and run the quick-start checklist this weekend
- Schedule a quarterly review

15 to 21: Bad Shape

Your exposure is real and exploitable by anyone willing to spend an afternoon. Start with the highest-impact items first: SIM swap defense, data broker removal, and account audit.

The Phone Privacy Guide handles the device layer end to end. The Wealth Privacy Stack (coming soon) handles the financial and asset layer.

If you have meaningful assets or specific concerns (stalker, professional exposure, post-divorce situation, public profile), this is the moment to bring in help. The work in front of you is significant and prioritization matters more than effort.

22 to 30: Critical Exposure

You're operating like an average person, which means you're a target waiting to happen. The work in front of you is significant and trying to do it all at once will burn you out and produce mistakes.

If you have any of the following, hire help instead of going it alone:

- Net worth over $1M
- A public profile or media presence
- A current or former stalker situation
- A divorce, custody dispute, or family situation with hostile parties
- A professional role where you're a target (executive, public figure, controversial industry)
- A history of being doxed or threatened

For everyone else at this level, the work is still doable solo but you should plan for it as a multi-month project, not a weekend.

NEXT STEPS

Regardless of your score, three actions are worth doing this week:

1. Set a carrier port-out PIN. Call your carrier. Tell them you want to add a port-out PIN or number lock. Pick a unique PIN that isn't your SSN, birthday, or address numbers. 15 minutes of work, kills the most common attack vector.

2. Audit your 2FA on critical accounts. Email, bank, brokerage, crypto exchanges, social media. If any of them use SMS, switch to authenticator app or hardware key. 1 hour of work, eliminates the SIM swap consequences.

3. Run a data broker opt-out pass. Either DIY through the top 10 sites (Spokeo, WhitePages, BeenVerified, Radaris, MyLife, PeopleFinder, Intelius, FastPeopleSearch, TruePeopleSearch, Nuwber) or use a paid service. This removes a year's worth of exposure in a weekend.

If you scored 15 or higher, your fourth action is to read the Phone Privacy Guide and start the device hardening. Your phone is the single highest-leverage privacy investment available to you.

THE BIGGER PICTURE

Privacy isn't a destination, it's a posture. The goal isn't invisibility. The goal is cost of attack.

The wealthy aren't private because no one knows they exist. The wealthy are private because finding them is expensive enough that almost no one bothers. Same logic applies to you. Every fix in this audit raises the cost of finding you, watching you, or attacking you.

The people who get hurt are the ones doing nothing. Average exposure, average defenses, average outcomes when things go wrong.

You took this audit, so you're already ahead of most. Don't let it stop here. Pick three items from your "yes" list and fix them this week. Come back to this audit in 90 days and re-score. Watch the number drop.

That's the whole game.

This audit is provided for educational purposes only. Privacy strategies evolve. Verify current best practices against authoritative sources before relying on specific recommendations. The author is not a licensed attorney and nothing in this document constitutes legal advice.