THE COMPLETE PHONE PRIVACY GUIDE

Hardening for iPhone and GrapheneOS

2025-2026 EDITION

by TRUCE

TABLE OF CONTENTS

PART 7 — MAINTENANCE

PART 1 — FOUNDATIONS

SECTION 1: WHY YOUR PHONE IS THE WHOLE GAME

If you only lock down one thing this year, lock down your phone.

Not your laptop. Not your social media. Not your home router. Your phone.

Your phone knows where you live, where you work, where you go on weekends, who you talk to, what you search at 2 AM, what you buy, how much you sleep, and roughly when you'll wake up tomorrow. It carries a microphone you never turn off, a camera that's always within reach, and a radio that broadcasts your exact location to a private company every few seconds. That company sells it.

Your computer goes to sleep when you walk away. Your phone is on you eighteen hours a day. The phone is the device.

Compromise the phone and you've compromised the email account on it, the banking app on it, the calendar showing your routine, the contacts showing your network, the photos showing your home, and the location history showing your patterns. One device, everything.

The hard truth: the phone makers, the carriers, and the app developers are not your adversaries the way a hacker is. They're worse. A hacker tries to break in. The companies in your phone already have the keys. They built the locks.

What this guide is

A phone-only guide. Two paths: hardening an iPhone, and switching to a Pixel running GrapheneOS. Both legitimate. Neither is "better" in an absolute sense, but the GrapheneOS path is the strongest option available today.

You won't get a chapter on email providers or VPN comparisons. Those belong in separate guides. The focus stays on the device.

What you actually gain

Your phone stops broadcasting your real-time location to companies that sell it. Your iCloud or Google account stops being a single point of failure. Your SMS messages stop being the second factor for your bank account, which closes off the single most common attack vector for wire fraud. Your phone, when stolen, becomes a brick. Your phone, when seized, doesn't immediately give up everything you've ever typed. Apps lose the ability to harvest your contacts, photos, and location for ad networks. And the people who actually want to find you find it takes them forty hours instead of forty cents.

That's the game. Not invisibility. 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.

Your phone is where this starts.

SECTION 2: CHOOSING YOUR PATH

Two paths. Pick one.

Path 1: The Hardened iPhone

What it is: keep your iPhone, set it up correctly, lock down the settings, change how you use it.

What it gets you: Advanced Data Protection encrypts most of your iCloud. Stolen Device Protection blocks the post-theft attack chain. Apple's hardware security (Secure Enclave, Face ID, T2 chip) is excellent. Compared to a default iPhone, this setup closes about 80% of the realistic privacy gap.

What it doesn't get you: independence from Apple. Apple still has metadata. Apple still gets your iCloud Mail, Contacts, and Calendar without end-to-end encryption. Apps can still do things you don't see at the OS level.

Difficulty: low. Most of the work is one weekend of careful setup. Quarterly audits after that.

Path 2: Pixel Plus GrapheneOS

What it is: buy a Google Pixel (unlocked, current generation), install GrapheneOS on it (an open-source privacy-hardened Android variant), use it as your daily device.

What it gets you: no Google by default. Granular network and sensor permissions per app (you can deny INTERNET access to any app, even Google Play Services). True multi-profile compartmentalization with separate encryption keys. A duress PIN that wipes the device if you're forced to unlock it. Auto-reboot to a more secure state after idle. USB-C data lockdown when locked. Verified open-source code.

What it doesn't get you: Apple ecosystem. Google Wallet contactless payments. Effortless setup. Some banking apps refuse to run (most work fine with Sandboxed Google Play, but verify yours).

Difficulty: medium. Installation takes 30-45 minutes the first time. Daily use is normal Android once configured.

The honest comparison

If you're serious about privacy and you have the willingness to learn something new, the Pixel plus GrapheneOS path is objectively the strongest setup available to a private individual.

The reason it isn't recommended to everyone is that most people aren't willing to do the small amount of upfront work. They don't want to learn a new OS. They don't want to verify their banking apps work. They want to stay in their Apple ecosystem because their family is on iMessage.

Those are valid reasons to stay on iPhone. They're just not technical reasons.

The combined approach

Some people run both. The iPhone stays in the daily rotation: family iMessage, banking, Apple Watch, AirPods. The Pixel running GrapheneOS handles anything sensitive: anonymous communications, separate identities, work that needs compartmentalization, financial accounts you don't want on the same

device as your photos.

We cover this in Section 23.

Make your choice

Look at the two paths. Pick.

If you're not ready for new infrastructure, do the hardened iPhone path.

If you want the strongest option, do the GrapheneOS path.

If you have the budget and the willingness, do both.

The rest of this guide assumes you've made a choice. Part 3 covers the iPhone setup. Part 4 covers the GrapheneOS setup. Parts 5 through 7 apply to both.

PART 2 — BUYING THE DEVICE

SECTION 3: BUYING A PHONE PRIVATELY

The privacy battle is lost or won at the point of sale. If you finance your phone through a carrier in your real name, with your real address on file, paid via your personal credit card, your device is tied to your identity before you even turn it on.

You can't undo a bad purchase. Start clean.

Rule 1: Buy unlocked. Always.

A carrier-locked phone is welded to the carrier you bought it from. You can't switch carriers without their permission. More importantly for GrapheneOS users: carrier-locked Pixels (especially Verizon SKUs) often refuse to allow bootloader unlock, which means you can't install GrapheneOS. Period.

Buy the unlocked SKU directly from Apple, the Google Store, B&H; Photo, or Best Buy (verify it's the unlocked model). If a price seems suspiciously good, the phone is probably carrier-locked.

For iPhone: buy direct from apple.com (filter to "Unlocked") or in-store. Avoid carrier offerings.

For Pixel: buy direct from store.google.com (filter to "Unlocked"), B&H;, or Best Buy's unlocked variant. Avoid the Verizon Pixel specifically; it blocks bootloader unlock.

Rule 2: Buy new. Not refurbished.

A refurbished phone is cheaper. It also went through unknown hands. There's no way to verify it wasn't tampered with at the hardware level. For privacy work, that's not a risk worth taking.

Rule 3: Pay anonymously where possible.

In order of preference:

Cash in store. Apple and Best Buy both accept cash. Walk in, pay cash, walk out. No card record, no credit check, no name on the transaction unless the purchase exceeds a threshold requiring ID.

B&H; Photo. They accept cash for in-person purchases at their NYC store, and they take Privacy.com cards online without the friction Apple sometimes has.

Privacy.com virtual card. If you must order online, use a Privacy.com card linked to your bank account. The card has whatever name you set on it. Apple sees a one-time-use card number. Your bank sees "Privacy.com" not "Apple." Set a one-time limit on the card.

LLC business card. If you have an LLC, buy through the LLC. The phone is a business expense, the card is in the LLC's name, the shipping address is your registered agent.

Worst case: a personal credit card. The phone is now tied to your real name forever in the manufacturer's records.

Rule 4: Get it shipped or picked up smart.

If you're paying cash and walking out with it: easiest. Done.

If you're shipping it: use a delivery address that isn't your home. A private mailbox at a UPS Store (they accept packages from any carrier), or your registered agent's address if you have an LLC.

Rule 5: Avoid carrier installment plans.

To finance through a carrier you have to give them your social security number, your full legal name, your home address, your employer, and your bank account for autopay. If you want privacy, pay outright.

Rule 6: Set it up at home, not in the store.

The store employees will encourage you to sign in with your existing accounts, enable iCloud, set up Significant Locations and a dozen other defaults you don't want.

Decline politely. Take the unboxed phone home. Set it up on your own Wi-Fi, with your own alias account, on your own time.

Rule 7: Skip the carrier setup.

Set up the phone BEFORE you put a carrier SIM in it. Initial setup on Wi-Fi only. Apply your privacy settings first. Then add the SIM.

For the GrapheneOS path:

Supported devices are listed in Section 12. For most people, the Pixel 9a or 10a is the sweet spot. Fully supported, 7-year update guarantee, and significantly cheaper than the Pro models. There's no reason to pay flagship prices for a privacy-focused use case.

PART 3 — THE HARDENED iPHONE

SECTION 4: INITIAL SETUP WITHOUT THE TRAPS

The first hour with a new iPhone determines the next three years of its privacy posture. Apple's Setup Assistant is designed to maximize the data you share with Apple. Every prompt has a default that's against your privacy interest.

Take an hour. Set it up like this.

Before you turn it on

You need: a Wi-Fi network you control, the Apple ID you're going to use (Section 5 covers creating this), and a list of the apps you actually use.

Do not have a SIM card in the phone yet. Setup on Wi-Fi only.

Do not connect this phone to a previous iPhone backup if your goal is a clean privacy reset. Restoring from backup brings over all your old app data, settings, and permissions. Set up as new.

During Setup Assistant

Language and region: pick your real region.

Quick Start: skip. Set up manually.

Wi-Fi: connect to your home network.

Touch ID / Face ID: enable. Biometrics are a security strength.

Create a passcode: tap "Passcode Options" and select "Custom Alphanumeric Code." Set a passphrase, not a 6-digit PIN. Six digits is brute-forceable. An alphanumeric passphrase of 12+ characters is not.

Apps & Data: "Don't Transfer Apps & Data."

Apple ID: sign in with your alias Apple ID (Section 5).

iMessage and FaceTime: enable if you'll use them.

Location Services: turn OFF for now. Re-enable selectively in Section 7.

Apple Pay: skip. Set up later if you want.

Siri: turn OFF. Siri records snippets of your voice and sends them to Apple servers.

Screen Time: skip.

App Analytics: "Don't Share."

iPhone Analytics: "Don't Share."

Immediately after setup

Don't open any apps yet. Don't connect a SIM yet. Open Settings:

Settings > Privacy & Security > Location Services. Confirm OFF.

Settings > Privacy & Security > Analytics & Improvements. Verify all toggles OFF.

Settings > Privacy & Security > Apple Advertising. Personalized Ads: OFF.

Settings > [your name] > iCloud. Disable everything you don't need. Section 6 covers the iCloud strategy in detail.

The Wi-Fi setting most people miss

Settings > Wi-Fi > tap the (i) next to your network > "Private Wi-Fi Address" set to "Rotating." This randomizes your MAC address per network. Without this, every Wi-Fi network you connect to logs a consistent unique identifier for your device.

This setting is per-network. Set it for each Wi-Fi you join.

SECTION 5: APPLE ID STRATEGY

Your Apple ID is the most important account in your digital life if you use an iPhone. If someone takes over your Apple ID, they take over your iPhone, your iPad, your Mac, and everything backed up to them.

Most people use the personal Apple ID they created at 19 with their real name, real email, real phone number, real birthday. That Apple ID has decades of purchase history, location data, photo backups, and personal information tied to it.

Two choices: rehabilitate the existing Apple ID, or start fresh with an alias.

The clean start: alias Apple ID

The right move for most people moving into a privacy-focused setup.

What you need:

A name. Doesn't have to be your real name. Doesn't have to be a fake name either. Many use a legitimate variation: middle name as first name, mother's maiden name as last name.

An email. Set up a Proton Mail or Tuta account with the alias name. Do NOT use Gmail.

A phone number. Use a VoIP number from VoIP.ms (Section 20). Do not use your real cell.

A birthday. Real birth year is fine. Different month and day is fine.

A payment method. Privacy.com card with the alias name. Apple will charge $1 to verify and refund it.

Setting up the alias Apple ID:

Do this BEFORE you start setting up the iPhone.

On a computer: go to appleid.apple.com and click "Create Your Apple ID." Use the alias information above. Verify the email. Verify the phone number (the VoIP number can receive verification SMS).

Set a strong password and write it down. Lose this password and you lose access to everything connected to this Apple ID.

Add a recovery contact and a recovery key. Recovery contact is someone you trust who has an iPhone. Recovery key is a 28-character string you write down and store in two physical locations.

Set up two-factor authentication using a hardware security key (YubiKey). Apple supports physical security keys for Apple ID 2FA. SMS 2FA on your Apple ID is one SIM swap away from total account takeover.

The existing Apple ID problem

If you've been using the same Apple ID for ten years with your real name, you have a choice: migrate to a new alias Apple ID (recommended) or aggressively scrub the existing one.

Migrating means setting up the new Apple ID, manually transferring what you want to keep, and abandoning the old one. You lose iCloud purchase history. App Store purchases are tied to the old Apple ID, but you can still re-download them if needed.

Scrubbing means going into Settings > [your name] and removing as much as possible. It's possible but you'll never get to a truly clean state.

For most people doing this seriously, the new alias Apple ID is the cleaner path.

The bottom line

Set up two-factor authentication with a hardware security key. Set up recovery contact and recovery key. Write down the password in two places. The most common privacy failure for iPhone users isn't Apple harvesting data. It's losing their Apple ID or being SIM-swapped into a takeover.

SECTION 6: ADVANCED DATA PROTECTION

Advanced Data Protection (ADP) is the single highest-impact iCloud setting Apple has ever shipped. If you do one thing in this guide, do this.

What it does

By default, your iCloud data is encrypted on Apple's servers, but Apple holds the encryption keys. They can decrypt your iCloud Photos, your iCloud Backup, your Notes, your Voice Memos, and dozens of other categories. They will do so under legal process. They will do so if their internal accounts are compromised.

With ADP enabled, you hold the keys. Apple cannot decrypt your data.

What ADP protects:

- iCloud Backup (the big one. Without ADP, your entire phone backup including iMessage history is decryptable by Apple)

- iCloud Photos
- iCloud Drive
- Notes, Reminders, Safari Bookmarks, Voice Memos, Wallet passes, Freeform
- Plus categories E2EE by default: Health, iMessage, Keychain, Maps, Memoji, Payment, QuickType, Safari history, Screen Time, Siri info, Wi-Fi passwords

What ADP does NOT protect (these stay decryptable by Apple even with ADP on, because they need to interoperate with global email/calendar standards):

- iCloud Mail
- Contacts
- Calendar

Do not store sensitive information in iCloud Mail, Contacts (notes fields on contacts especially), or Calendar. Move sensitive info to Proton or Tuta.

Critical: ADP is not available in the UK

Apple withdrew ADP for UK users after the UK government issued an order demanding a backdoor. If you're a UK resident, you cannot enable ADP. Use Signal for everything sensitive, use Proton for email, use a non-iCloud backup method.

Before you enable ADP

ADP requires that you set up account recovery FIRST. Apple cannot help you if you lose access. The encryption keys are on your devices and in your recovery materials.

Set up:

A Recovery Contact. Someone you trust with an iPhone. Pick someone reachable years from now.

A Recovery Key. A 28-character code. Write it down. Store it in two physical locations that aren't co-located (one in your home safe, one in a safe deposit box). Do NOT store it in iCloud, Notes, or any cloud service.

If you don't set these up, ADP will refuse to enable.

Enabling ADP

Settings > [your name] > iCloud > Advanced Data Protection > Turn On Advanced Data Protection.

Apple walks you through verifying your recovery contact and recovery key. The re-encryption can take a few hours. Plug your phone in and let it run.

Verifying ADP is on

Settings > [your name] > iCloud > Advanced Data Protection should show "On."

Settings > [your name] > iCloud > See All. Each category protected by ADP shows "End-to-End Encrypted."

iMessage in iCloud

If you sync iMessage to iCloud, this only stays end-to-end encrypted with ADP on. Without ADP, the iMessage backup in your iCloud Backup is decryptable by Apple, which breaks iMessage's E2EE for backup purposes.

Sync iMessage to iCloud: Settings > [your name] > iCloud > Messages > toggle on.

The one risk

If you lose both your recovery contact and your recovery key, your iCloud data is unrecoverable. Apple cannot help. The Genius Bar cannot help. This is the price of true end-to-end encryption. Write down the recovery key. Do not lose it.

SECTION 7: THE COMPLETE SETTINGS CHECKLIST

This is the section you'll bookmark and come back to. Work through it once at setup, then revisit quarterly. iOS updates occasionally reset some toggles.

Settings > [your name]

Name & Phone Numbers: review. Should match your alias Apple ID.

Password & Security: 2FA on, hardware security key configured.

Subscriptions: cancel anything you're not using.

Settings > Wi-Fi / Bluetooth / Cellular

Wi-Fi: tap (i) on the network, set Private Wi-Fi Address to Rotating. Auto-Join Hotspot: Never.

Bluetooth: turn off when not actively using.

Cellular: scroll to bottom > Wi-Fi Assist OFF.

Settings > Notifications

Show Previews: When Unlocked or Never. Default is "Always" which means lock screen previews show your messages to anyone who picks up your phone.

Per-app notifications: be aggressive. Most apps don't need notifications.

Settings > General > AirDrop

Receiving Off, or Contacts Only at most.

Settings > General > Background App Refresh

Off, or Wi-Fi only. Most apps refresh in the background to stay current, which means they're running and tracking even when you're not using them.

Settings > General > VPN & Device Management

Should be empty unless you've installed a VPN configuration profile. If anything's here you didn't install, remove it immediately.

Settings > Display & Brightness > Auto-Lock

30 seconds or 1 minute.

Settings > Search

Show in Look Up: OFF Show in Spotlight: OFF for everything you don't need Siri Suggestions in App: OFF Siri Suggestions while Searching: OFF Show on Lock Screen: OFF

Settings > Face ID & Passcode

Turn ON: Require Attention for Face ID Turn ON: Attention Aware Features Turn OFF: Voice Dial

Allow Access When Locked: turn OFF everything you don't need. Specifically: Today View, Notification Center, Control Center, Siri, Reply with Message, Home Control, Wallet, Return Missed Calls, USB Accessories.

Erase Data after 10 failed attempts: turn ON.

Settings > Emergency SOS

Call with 5 Button Presses: ON. Lets you trigger Emergency SOS without unlocking. Also useful because pressing the side button 5 times disables Face ID until you re-enter your passcode (the biometric lockout gesture from Section 10).

Settings > Privacy & Security

The most important menu in the entire phone.

Location Services: On, but every app should be reviewed. Set most apps to "Never" or "Ask Next Time." Only Maps, Weather, and apps you actively use for location should be "While Using the App." None should be "Always" unless they have a specific reason.

Location Services > System Services: turn OFF Significant Locations (and clear history), iPhone Analytics, Routing & Traffic, Improve Maps, Location-Based Suggestions, Location-Based Alerts, Location-Based Ads.

Tracking: "Allow Apps to Request to Track" OFF.

Apple Advertising: Personalized Ads OFF.

Analytics & Improvements: all OFF.

App Privacy Report: turn ON to see what apps are doing.

Per-category permission audit

In Privacy & Security, scroll up. Each category lists apps that have requested access:

Contacts: remove anything that doesn't need contacts. Social media apps and games never need your contacts.

Calendars, Reminders, Photos, Bluetooth, Microphone, Camera, Speech Recognition, Local Network, Nearby Interactions, Motion & Fitness, Focus, Sensors: review each. Deny anything that doesn't need it.

This audit is tedious. Do it once carefully. You'll be amazed how many apps have permissions they don't need.

Settings > Safari

Search Engine: DuckDuckGo or Brave Search.

Search Engine Suggestions: OFF (sends every keystroke to the search engine).

Safari Suggestions: OFF.

Privacy & Security:

- Prevent Cross-Site Tracking: ON
- Require Face ID/Touch ID to Unlock Private Browsing: ON
- Hide IP Address: From Trackers and Websites
- Advanced Tracking and Fingerprinting Protection: All Browsing
- Privacy Preserving Ad Measurement: OFF

Block Pop-ups: ON.

Camera, Microphone, Location: All Deny by default.

Settings > Mail

Privacy Protection: Protect Mail Activity ON. Routes mail through proxy servers, hiding your IP from senders and defeating tracking pixels.

Settings > Messages

Send Read Receipts: OFF.

iMessage Apps: turn off ones you don't use.

Settings > Photos

Shared Albums: OFF unless you actively share albums.

iCloud Photos: ON if you have ADP enabled.

Settings > Wallet & Apple Pay

Allow Access When Locked: turn OFF Double-Click Side Button.

Settings > Apps

For each app, review its permissions. Be aggressive. Special attention to: Facebook, Instagram, TikTok, Snapchat, X, LinkedIn, dating apps. All aggressively harvest data. Either delete them or lock down their access entirely.

SECTION 8: STOLEN DEVICE PROTECTION

This is the iOS feature that prevents the post-theft attack chain. If you skip everything else in this guide, do this.

The attack pattern

Thieves watch you type your iPhone passcode in a public place (gym, bar, restaurant), then steal the phone. With your passcode, they open Settings, change your Apple ID password, lock you out of iCloud, and have access to your photos, contacts, messages, and Keychain (all your saved passwords). They drain accounts in under an hour.

What Stolen Device Protection does

When enabled, sensitive actions require Face ID or Touch ID with no passcode fallback. The thief can't bypass biometrics with the passcode they shoulder-surfed.

Some actions also require a one-hour Security Delay. After authenticating once, you wait an hour, then authenticate again. This delay gives the legitimate owner time to notice the phone is gone and remote-wipe it via Find My before the thief can change the Apple ID password.

Protected actions include: changing the Apple ID password, changing your iPhone passcode, removing Face ID or Touch ID, disabling Find My, erasing all content, using saved passwords from Keychain, using stored payment methods.

The critical setting: set to Always

When you enable SDP, iOS asks: only when away from familiar locations (home, work), or Always?

Default is "Away from Familiar Locations." Don't leave it there.

Set it to Always.

The Familiar Locations option means SDP is off when you're at home or work. Your phone is stolen at your gym down the street from your apartment? SDP doesn't protect you. Your phone is taken from your home during a burglary? SDP doesn't protect you.

Set it to Always. The 1-hour delay is a minor inconvenience when you're at home. The protection it provides when you're in public is non-negotiable.

Enabling Stolen Device Protection

Requirements: two-factor authentication on Apple ID, device passcode set, Significant Locations on, Face ID or Touch ID set up.

Settings > Face ID & Passcode > scroll down to Stolen Device Protection > Turn On.

Then: Stolen Device Protection > Require Security Delay > Always.

Note: on recent iOS versions, Stolen Device Protection may already be on by default. Verify the setting is on, and verify the Security Delay is set to Always (not the default "Away from Familiar Locations").

Pair SDP with Find My

SDP only buys you time. You still need to remote-wipe the phone to fully protect your data after a theft.

Settings > [your name] > Find My > Find My iPhone > ON. Enable: Find My network, Send Last Location.

Practice this once: from a friend's phone or icloud.com, log into your Apple ID and try the Find My feature. Know the steps before you need them.

SECTION 9: LOCKDOWN MODE

Lockdown Mode is Apple's "optional, extreme" protection for people specifically targeted by state-level mercenary spyware.

Who needs it

Most people don't. The friction outweighs the benefit for normal threat models.

You need Lockdown Mode if:

- You've received an Apple Threat Notification (Apple proactively warns users they believe are targeted by state actors)
- You're a journalist, activist, dissident, or human rights worker in or from a country with active surveillance programs
- You work on sensitive national security matters
- You're a public figure with documented stalker problems
- You travel to or from countries with high mercenary spyware activity

What it does

Lockdown Mode disables features that have been exploited in past spyware attacks. Specifically:

- Disables most iMessage attachment types (photos still work)
- Disables link previews in Messages

- Disables web technologies in Safari like just-in-time JavaScript compilation, which makes some sites slower or broken
- Blocks incoming FaceTime calls from people you've never called
- Blocks Wi-Fi joins to non-secure networks
- Turns off 2G/3G cellular (forces 4G/5G only)
- Blocks USB connections to a computer when the phone is locked
- Blocks configuration profiles (MDM, VPN config profiles, certificates)

The cost

Lockdown Mode breaks things. Some websites won't work properly. Some message attachments won't open. You can't receive FaceTime from someone you've never called. You can't auto-join open Wi-Fi. Some banking apps that rely on advanced web features may break.

For everyday use, this friction is significant. For high-risk users, it's worth it.

Enabling Lockdown Mode

Settings > Privacy & Security > Lockdown Mode > Turn On Lockdown Mode.

The phone restarts. You can turn it off at any time.

If you receive an Apple Threat Notification, enable Lockdown Mode immediately and contact a professional to assess your full setup.

SECTION 10: PHYSICAL SECURITY

Most phone privacy guides ignore physical security. They focus on apps and settings. But every threat model has a physical layer: what happens if someone has hands on your phone for thirty seconds, or thirty minutes, or thirty days.

Your passcode

Use an alphanumeric passcode. Not a 6-digit PIN, not a 4-digit PIN, not a swipe pattern. 12+ characters mixed case with at least one symbol.

A 4-digit PIN has 10,000 combinations and can be brute-forced in minutes if the phone is in a vulnerable state.

A 6-digit PIN has 1 million combinations. Better, but still tractable for state-level tools.

A 12-character alphanumeric passphrase has roughly 6.1 quintillion combinations. Even nation-state forensic tools fail against this in practical timeframes.

Use Face ID or Touch ID for normal unlock. The passphrase is for the moments biometrics fail or you need to unlock cold.

Memorize it. Don't write it down anywhere a thief could find. If you must write it down, lock it in a safe.

Biometrics vs passcode: the legal nuance

In the U.S., the Fifth Amendment generally protects against being compelled to reveal a passcode (because revealing it requires you to use your mind, which is testimony).

Biometrics have been treated differently. Most courts have ruled that police can compel you to place your finger on the sensor or look at the phone for Face ID, because this doesn't require you to "testify." You're providing a physical sample.

The biometric lockout gesture

You can disable Face ID temporarily with a gesture. Press and hold the side button and either volume button for two seconds. The "slide to power off" / "Emergency SOS" screen appears. Cancel out, and now your phone requires the passcode (not Face ID or Touch ID) for the next unlock.

Practice this gesture. If you're ever in a situation where you might be compelled to unlock by biometrics (traffic stop, arrest), execute the gesture before handing over the phone.

After 48 hours of no biometric unlock, the phone automatically falls back to passcode-only. Built-in protection.

Auto-Erase

Settings > Face ID & Passcode > Erase Data: ON.

After 10 failed passcode attempts, the device wipes.

Inactivity reboot

Recent iPhones automatically reboot after extended idle time. The reboot puts the phone into the Before First Unlock (BFU) state, which is harder for forensic tools to extract data from.

This is on by default. Don't disable it.

Why it matters: in the After First Unlock (AFU) state, forensic tools have higher success rates against various iOS versions. In the BFU state (cold boot, no unlock since), success rates drop significantly.

For high-risk users: reboot your phone regularly. Weekly manual reboots keep the phone closer to the BFU state more of the time.

Find My

Settings > [your name] > Find My > Find My iPhone ON, with Find My network on and Send Last Location on.

Practice remote-wiping from icloud.com or a friend's device. Know the steps before you need them.

USB / Lightning data

Settings > Face ID & Passcode > Accessories (under "Allow Access When Locked") > "USB Accessories" OFF. Disables USB data access when the phone has been locked for more than an hour.

Combined with the inactivity reboot, this significantly reduces the forensic attack surface.

Carrying it

Don't leave it on tables at restaurants. Don't leave it in a gym locker without knowing the locker is secure. Don't lend it to strangers to "make a quick call" (a documented pickpocket pattern).

The bottom line

The settings you spent an hour configuring don't matter if your phone is in someone else's hands with a known passcode.

Alphanumeric passcode. Auto-erase on. Stolen Device Protection on Always. Biometric lockout gesture practiced. Find My set up and tested. Inactivity reboot on. USB Accessories off when locked.

That's the iPhone hardening complete.

PART 4 — THE GRAPHENEOS PIXEL

SECTION 11: WHY GRAPHENEOS IS THE BEST OPTION

If privacy actually matters to you, this is the answer. Not a hardened iPhone. A Pixel running GrapheneOS.

The Privacy Guides team lists it as their top mobile recommendation. The OPSEC community treats it as the floor for serious work, not the ceiling. Here's what it actually gets you.

No Google by default

A normal Android phone is a Google product. Google sees your location, your searches, your apps, your account activity, your contacts, your calendar, your messages (if you use Google Messages), your photos (if you use Google Photos), and roughly everything else you do. They monetize all of it.

GrapheneOS ships with no Google apps or services. The default browser is Vanadium (a hardened Chromium fork with no Google calls). The default app store is the GrapheneOS App Store and F-Droid. No Google Play Services running in the background, no Google Mobile Services scanning your apps, no Google Location Services pinging your GPS.

If you want Google Play (so you can run apps that need it), you can install Sandboxed Google Play into a profile. Section 17 covers that. Google runs as a normal app with no special privileges, in a sandbox you control.

Granular network permission per app

This is the killer feature no other consumer OS has.

In GrapheneOS, every app's INTERNET permission is a toggle you can revoke at any time. Per app. At any time. You can grant an app permission to your camera and microphone but deny it network access. The app cannot phone home. The app cannot send your data anywhere.

On iOS, on stock Android, and on macOS, network access is implicit. An app that has permission to run has permission to talk to the internet. GrapheneOS makes this an explicit, revocable permission per app.

This single feature changes how you think about apps. That weird tip calculator that asks for permissions you don't understand? Deny network access. The flashlight app that wants to "phone home"? Deny network access.

Granular sensor permissions

Similar story. Deny apps access to sensors (gyroscope, accelerometer, compass, barometer) without affecting any other permission. Most apps that ask for sensor access are doing it for fingerprinting or behavioral tracking.

User profiles with separate encryption keys

GrapheneOS supports multiple user profiles on one device. Each profile has its own encryption key. Each profile is essentially a separate phone. Apps installed in one profile don't see apps in another. Files in one profile aren't accessible from another.

This enables real compartmentalization. We cover the setups in Section 14.

Duress PIN

You set two PINs (or passwords): your real one, and a duress one. If you ever enter the duress PIN, the device immediately and irreversibly wipes itself. No warning, no prompt. The wipe begins instantly.

This protects against forced unlock scenarios. Border agent, mugger, abusive partner, anyone who can compel you to unlock the device. You enter the duress PIN. Device wipes.

Auto-reboot

Configurable auto-reboot to the BFU (Before First Unlock) state after a set idle period. Default is 18 hours. You can set it to as little as a few minutes. The BFU state is much harder to extract data from with forensic tools.

USB-C data lockdown

When the phone is locked, USB-C is set to charging only at the hardware level. No data lines active. Forensic tools that connect via USB get nothing.

Verified open source

GrapheneOS is open source. Anyone can audit the code. Researchers and security professionals do, regularly. The privacy claims are verifiable, not just marketing language.

Hardware security

GrapheneOS only runs on Google Pixel devices. Pixels have the Titan M2 secure element, hardware-backed verified boot, and (Pixel 8 and later) ARM memory tagging (MTE) which mitigates whole classes of memory corruption exploits.

The combination of GrapheneOS software hardening and Pixel hardware security is the strongest mobile security platform available to a civilian.

What you give up

iMessage (Apple-only). FaceTime (Apple-only). Apple Watch (Apple-only). Apple Pay (Google Wallet works on stock Android but not GrapheneOS due to Google's Play Integrity requirements). Some banking apps that aggressively enforce Google Play Integrity will refuse to run (most work fine with Sandboxed Google Play, but verify yours).

The user experience is normal Android. If you've used Android, you'll be at home in 15 minutes. If you've only used iPhone, expect a few days of adjustment.

The bottom line

This is the strongest option. If you're serious about privacy, this is the device you want.

If you want one of these phones already configured, fully private, done for you, ready to use with instructions for anything regarding the phone, DM @truce_privacy.

SECTION 12: BUYING THE RIGHT PIXEL

Not every Pixel works with GrapheneOS. Some carrier-locked Pixels won't allow bootloader unlock. Some older Pixels are out of support.

Supported devices

GrapheneOS officially supports:

- Pixel 6, 6 Pro, 6a (end of life approaching, get a newer model if buying now)
- Pixel 7, 7 Pro, 7a
- Pixel Tablet
- Pixel Fold
- Pixel 8, 8 Pro, 8a
- Pixel 9, 9 Pro, 9 Pro XL, 9 Pro Fold, 9a
- Pixel 10, 10 Pro, 10 Pro XL, 10 Pro Fold, 10a

Older Pixels (5 and earlier) are no longer supported.

My recommendation: Pixel 9a or 10a

Both are fully supported. Both get the 7-year update commitment from Google. Both have the Titan M2 secure element and ARM MTE. Both are significantly cheaper than the Pro models.

The Pro models offer better cameras and larger screens but the privacy capabilities are identical. Save the money and buy the a-series.

Why Pixel 8 and later specifically

Two reasons:

1. 7-year update commitment. Pixel 8 and later receive 7 years of security and OS updates from Google. Older Pixels get less.

2. ARM MTE (Memory Tagging Extension). Pixel 8 and later support this hardware feature. GrapheneOS uses it by default to mitigate memory corruption exploits, the primary attack vector for zero-day spyware.

Where to buy

In order of preference:

1. **Google Store directly (store.google.com)**. Filter to "Unlocked." Pay with Privacy.com card or business card. Ship to a non-home address.

2. **Best Buy unlocked**. Verify it's the unlocked SKU. Cash works in store.

3. **B&H; Photo**. Solid for cash purchases.

4. **Amazon (with caution)**. Verify seller is Amazon directly, not a third-party.

Avoid:

• Verizon-locked Pixels. Verizon blocks bootloader unlock on Pixel SKUs, which makes GrapheneOS uninstallable.

• AT&T; or T-Mobile carrier financing. Creates an identity trail.

• eBay or Facebook Marketplace. Used Pixels could be reported lost or stolen, in which case Google will eventually brick the activation lock.

Verify before you flash

1. Power it on. Go through initial setup just enough to verify it works. Connect to Wi-Fi.

2. Settings > About Phone > Build Number. Tap "Build Number" seven times to enable Developer Options.

3. Settings > System > Developer Options > OEM Unlocking. Verify this toggle is available (not greyed out). If it's greyed out, the phone is carrier-locked and you cannot install GrapheneOS. Return it.

4. Run the GrapheneOS installer's hardware check at install.grapheneos.org.

5. Factory reset the phone (Settings > System > Reset Options > Erase All Data).

Storage choice

128GB is fine for a privacy device. 256GB if you want headroom. Don't pay for 512GB or 1TB unless you have a specific reason.

SECTION 13: INSTALLATION WALKTHROUGH

You can install GrapheneOS yourself. It takes 30-45 minutes for a first-timer. The official web installer at install.grapheneos.org handles everything via a browser. No command line needed.

What you need

- A Pixel that supports GrapheneOS
- A computer running Chromium-based browser (Chrome, Brave, Edge) or Firefox
- A high-quality USB-C cable that supports data
- About 45 minutes of uninterrupted time

Step 1: Enable Developer Options and OEM Unlocking

On the Pixel:

1. Settings > About Phone > tap "Build Number" seven times.
2. Settings > System > Developer Options > OEM Unlocking > toggle ON.
3. Verify OEM Unlocking is on. If greyed out, your Pixel is carrier-locked and cannot install GrapheneOS.

Step 2: Open the web installer

On the computer, open Chromium or Firefox and go to install.grapheneos.org. Connect the Pixel to the computer with the USB-C cable.

Step 3: Unlock the bootloader

The web installer walks you through this. The Pixel reboots into bootloader mode. The installer sends the unlock command. The Pixel displays a warning screen. Confirm with the volume button to highlight "Unlock the bootloader" and press power to select.

The phone wipes itself. This is normal.

Step 4: Flash GrapheneOS

The web installer downloads the latest stable build and flashes it. Takes 5-10 minutes. Don't disconnect the cable.

Step 5: Lock the bootloader

THIS IS CRITICAL. After flashing GrapheneOS, you must re-lock the bootloader.

A locked bootloader enables verified boot, which cryptographically verifies the OS hasn't been tampered with on every boot. An unlocked bootloader is a significant security downgrade.

The web installer prompts you to lock the bootloader at the end of installation. Confirm.

Locked bootloader + GrapheneOS = secure setup. Unlocked bootloader + GrapheneOS = insecure setup. Don't ship it like this.

Step 6: First boot

The Pixel boots into GrapheneOS. Walk through the setup:

- Language and region
- Wi-Fi connection
- Date and time
- Owner profile: set a strong alphanumeric passcode (12+ characters)
- Set up fingerprint if you want

Step 7: Verify

Settings > About Phone. Build Number should include "GrapheneOS."

Settings > Security > Encryption & Credentials. Device is encrypted.

You're running GrapheneOS.

Common issues

OEM Unlock greyed out: phone is carrier-locked. Return it.

Web installer fails to detect device: try a different USB-C cable, USB port, or browser.

Bootloader unlock fails: phone may be carrier-locked despite saying it's unlocked.

Bricked phone after install: very rare. GrapheneOS provides a recovery path via the same web installer.

If you want one of these phones already configured, fully private, done for you, ready to use with instructions for anything regarding the phone, DM @truce_privacy.

SECTION 14: USER PROFILES AND COMPARTMENTALIZATION

Profiles are GrapheneOS's killer feature for serious privacy work. They give you what amounts to multiple phones on one device, each with its own encryption key.

Why this matters

A single user account on a phone is a single point of failure. If one app is compromised, it can attempt to access data from other apps on the same profile. If you're forced to unlock the phone, you reveal everything on it. If you install an app you don't fully trust, it shares the system with apps you do trust.

Profiles solve this. Each profile is its own isolated environment. Apps in one profile can't see apps in another. Data in one profile can't be accessed from another. Even at the kernel level, profiles are separated.

The profile structure

The "Owner" profile is the primary administrative profile. Always present. Some system functions can only be done from Owner.

You can create additional profiles. The Owner can create, switch to, or delete other profiles. Other profiles can't see or affect each other.

Setup options

Light: Owner profile + one "Daily" profile. Owner stays minimal. Daily has your everyday apps. Useful if you want some compartmentalization without managing many profiles.

Work/personal split: Owner (admin only) + Personal (family contacts, banking, photos) + Work (work apps, email, contacts). Good for business owners.

Full compartmentalization: Owner (admin only) + Personal (family, banking, daily) + Work (work apps) + Sensitive (encrypted comms, anonymous email) + Google (Sandboxed Google Play installed here only). Maximum isolation.

Setting up profiles

Settings > System > Multiple Users > Add User.

Each new profile gets a name, its own apps, its own settings, its own encryption key, its own data.

To switch profiles: from the lock screen, swipe down on the notification area, tap the profile icon (top right) to switch.

The "Google" profile pattern

A common configuration: create a profile specifically for Google services. Install Sandboxed Google Play in that profile (Section 17). Install any apps that require Google Play Services in that profile. Use that profile only when needed.

For the rest of your daily life, you're in your Personal or Work profile, which has no Google services running.

Storage Scopes and Contact Scopes

Storage Scopes: instead of granting an app access to your entire file system, grant access to specific files or folders.

Contact Scopes: instead of "this app can see all my contacts," say "this app can see these three contacts" or "this app can see a fake empty contact list."

These features are unique to GrapheneOS and they're powerful. They let you give apps just enough access to function without giving them full access.

Maintenance

Quarterly, review each profile and clean out apps you no longer use.

If a profile gets compromised or you want to start fresh, you can delete the profile. The encryption key is destroyed. The profile's data is unrecoverable.

SECTION 15: NETWORK AND SENSOR PERMISSIONS

This is where GrapheneOS shows its most obvious advantage over iOS and stock Android. Every app's access to the network and to device sensors is a revocable permission.

The INTERNET permission

In stock Android and iOS, when an app is installed, it has implicit network access. The user has no way to deny this.

In GrapheneOS, INTERNET is treated as a regular permission you can grant or revoke. Per app. At any time.

Settings > Apps > [app name] > Permissions > Network. Toggle off and the app cannot connect to the internet.

Use cases

Apps that don't need internet but ask for it anyway: tip calculators, flashlight apps, simple games, photo editors, calculator apps, file viewers, ebook readers. Almost none of these need network access. Their network access exists only to phone home with analytics, push tracking SDKs, or serve ads. Deny network access. The app still works.

Banking apps: do need network access. Leave on.

Camera apps: don't need network access. Photos stay on device.

Note apps: most don't need network unless you're syncing.

Music players that play local files: don't need network.

Sandboxed Google Play: can have network access denied if you only want to use Google Play to install apps and then immediately deny.

Routine network audit

Every quarter, go through your installed apps. For each one ask: does this app need the internet?

You'll find that 30-40% of your apps don't need network access. Revoking it makes them safer (they can't leak data, can't track you remotely) and slightly improves battery.

Sensor permissions

Similar story for sensors. The Sensors permission covers the gyroscope, accelerometer, compass, barometer, ambient light sensor, and similar.

Most apps don't need sensor access. They request it for fingerprinting (sensor noise patterns can identify a specific device), behavioral analytics, or because their SDK developer included it.

Settings > Privacy > Permission Manager > Sensors. Deny sensors for apps that don't need them.

Microphone, camera, location

Standard Android permissions, but GrapheneOS adds an indicator in the status bar when any app is using them. If you see the indicator and you're not actively using an app that should have access, investigate.

Location: GrapheneOS lets you grant approximate location (city-level) instead of precise location for most apps. Use this aggressively. Banking apps don't need precise location. Weather apps don't need precise location.

Bottom line

Spend an afternoon going through every app on your GrapheneOS device. For each one, ask: does it need this permission?

In ninety percent of cases, the answer is no for at least one permission. Revoke it.

SECTION 16: DURESS PIN, AUTO-REBOOT, USB-C LOCKDOWN

Three GrapheneOS-specific features that handle threats no other consumer OS handles.

Duress PIN

Settings > Security > Device unlock > Duress password.

Set a second password (or PIN). When that password is entered anywhere the device asks for unlock (lock screen, app prompts), the device immediately and irreversibly wipes.

The wipe is fast. You can't undo it. There's no "confirm" prompt. Enter the duress PIN, the device starts wiping.

Use cases

Mugging. Someone demands your phone and your unlock. You comply with the duress PIN. They get a wiping phone.

Forced unlock by an abusive partner, family member, or anyone with physical control over you. Same principle.

A break-in or home invasion where you're cornered and someone has leverage to compel you. The duress PIN gives you a way out that looks like compliance.

Important notes about duress PIN

Once set, you must remember both PINs. Mixing them up means accidentally wiping your phone. Don't make them similar.

The duress PIN wipes the device including all profiles. The wipe is irreversible. If you have important data on the device that you don't have backed up elsewhere, the duress PIN destroys it permanently.

This is a power-user feature. Don't enable it casually.

Auto-reboot

Settings > Security > Auto reboot.

After a configurable idle period, the device automatically reboots into the BFU (Before First Unlock) state. The BFU state is significantly harder for forensic tools to extract data from.

Default is 18 hours. Can set it as low as a few minutes or as high as 72 hours.

For most users: 18 hours is reasonable. For high-risk users: 4-6 hours.

Auto-reboot resets when you unlock the phone. If you use your phone throughout the day, you may never hit the threshold. But overnight when you're sleeping, the phone reboots into BFU.

USB-C lockdown

Settings > Security > USB-C.

Options:

- Charging-only when locked (default and recommended): USB data pins disabled when locked. Forensic tools that connect via USB get no data access.
- Charging-only always: USB never carries data.
- Disabled when locked: USB port fully disabled when locked. Even charging fails.

For most users: charging-only when locked.

PIN scrambling

Settings > Security > Device unlock > Scramble PIN keypad.

When entering your PIN, the digits are scrambled into a random arrangement instead of the standard 0-9 grid. Defeats shoulder-surfing.

If you use an alphanumeric password (you should), this matters less.

The combined effect

Strong alphanumeric passphrase. Duress PIN if your situation warrants it. Auto-reboot at 6-18 hours. USB-C charging-only when locked. PIN scramble if you use numeric.

A phone configured this way is a brick to anyone who steals it. None of this is available on iOS.

SECTION 17: SANDBOXED GOOGLE PLAY AND BANKING

The single most common GrapheneOS question: "but will my banking app work?"

Usually yes. Often without Sandboxed Google Play. Sometimes you need Sandboxed Google Play. Rarely the bank's app won't work no matter what you do.

What Sandboxed Google Play is

GrapheneOS lets you install the real Google Play Services and Google Play Store as regular apps. They run in a sandbox with no special privileges. They don't have system-level access. They don't run constantly in the background.

Compare to stock Android, where Google Play Services is a system app with deep integration, runs constantly, and is privileged.

Sandboxed Google Play is the same software running with no special privileges. It can do what it needs to do but it can't see things you don't explicitly allow.

When you need it

Banking apps that enforce Play Integrity (a Google service that checks if the device is "trusted"). Many U.S. and European banks require this. If a bank app refuses to open and you see "device not supported" or "rooted device detected," you probably need Sandboxed Google Play.

Apps that rely on Firebase Cloud Messaging for push notifications: Signal, WhatsApp, Discord. They work without Google Play Services if you configure UnifiedPush or accept delayed notifications. Easier path is Sandboxed Google Play.

Apps that require Google Wallet or Google Pay specifically: probably won't work even with Sandboxed Google Play, because these features require system-level integration.

Installing Sandboxed Google Play

In the profile where you want Google services (typically a dedicated "Google" profile):

1. Open the GrapheneOS App Store (preinstalled).
2. Install "Google Play services."
3. Install "Google Services Framework."
4. Install "Google Play Store."

Open the Play Store, sign in with a Google account (use an alias account, not your real one), and install whatever apps you need.

The compatibility tracker

Before assuming an app won't work, check the community-maintained banking apps compatibility report. Search "GrapheneOS banking compatibility." The community tracks which banks work, which require Sandboxed Google Play, and which refuse entirely.

Most U.S. and European banks work fine with Sandboxed Google Play. A few banks in certain countries with strict app attestation won't work at all. In that case, use the bank's web interface in a browser.

Other Google-dependent apps

Uber, Lyft, DoorDash, Instacart: work fine with Sandboxed Google Play.

YouTube, Gmail, Google Drive: work fine. You can also use NewPipe (FOSS YouTube client) without any Google services.

Google Authenticator: don't use it. Use Aegis (FOSS, exports to encrypted backups) for TOTP codes instead.

Google Password Manager: don't use it. Use Bitwarden instead.

Google Photos: don't use it. Use Aves or a local-only solution.

Apps that flag "rooted device"

Some apps detect environments they consider risky and refuse to run. GrapheneOS isn't rooted, but some apps' detection logic flags it anyway.

Common culprits: some banking apps, some streaming services (Netflix sometimes works, sometimes doesn't), some games with anti-cheat.

If an app refuses, options are: use the web version, find an alternative app, or accept it isn't available to you.

Bottom line

Sandboxed Google Play makes GrapheneOS practical for daily use without sacrificing the privacy gains. Set up a dedicated profile for Google services. Use it when you need Google-dependent apps. Stay in your other profiles the rest of the time.

PART 5 — THE CELLULAR LAYER

SECTION 18: SIM SWAP DEFENSE

If you only do two things from this entire guide: enable Stolen Device Protection and set up SIM swap defense.

A SIM swap is when an attacker convinces your carrier to move your phone number to a SIM card they control. Once they have your number, they receive your SMS 2FA codes. With your SMS codes, they reset your email password. With your email, they reset your bank password. They drain accounts in under an hour.

How SIM swaps work

The attacker calls your carrier. They impersonate you. They have some of your personal info, often pulled from data breaches or data brokers.

The carrier rep, under pressure to provide customer service, transfers the number to a new SIM. Sometimes this is a physical SIM at a store. Increasingly, it's a remote eSIM QR code, which the rep can issue from their terminal without ever meeting the "customer" in person.

Within minutes, you lose service. Within an hour, your bank accounts and email may be compromised.

The defenses

1. Carrier number lock (port-out protection)

Every major U.S. carrier offers a "number lock" or "port-out PIN" to prevent unauthorized number transfers.

T-Mobile: "Account Take Over Protection" or "NOPORT." Set via T-Mobile app or by calling.

Verizon: "Number Lock." Found in My Verizon app under account settings.

AT&T;: "Wireless Account Lock" or set a passcode specifically for porting requests.

Pick a unique PIN that's not your address number, social security number, or birthday. Write it down somewhere secure.

Caveat: these locks aren't bulletproof. Carrier reps can be social-engineered into bypassing them. But the lock adds friction. An attacker working through 50 numbers skips the locked ones for easier targets.

2. Get off SMS 2FA entirely

The lock makes a SIM swap harder. Getting off SMS 2FA makes a SIM swap irrelevant.

Switch to:

- Hardware security key (YubiKey or similar). The gold standard. Phishing-proof. SIM-swap-proof. Use for email, banking, crypto exchanges, any account that holds significant value.

- Authenticator app TOTP codes. Aegis on Android (open source), Raivo on iOS, or Authy if you must. Codes generated on your device. SIM swap can't get them.

- Passkeys (FIDO2). Apple, Google, and Microsoft all support these. Cryptographic, device-bound, phishing-proof.

Audit every account with 2FA. If it's SMS, switch it. Especially:

- Primary email
- All banking accounts
- Investment and brokerage accounts
- Crypto exchanges
- Social media (X/Twitter accounts have been hijacked via SIM swaps repeatedly)
- Cloud storage
- Domain registrar accounts (if someone takes your domain, they take your email)

3. Remove your phone number from accounts that don't need it

Most services aggressively prompt you to add a phone number "for security." Then they use it as a recovery vector that bypasses your 2FA.

Audit every account: does this service have a phone number on file? Do they need it?

For most accounts, you can remove the phone number entirely. For some that require one, use a VoIP number (Section 20), not your real cell.

The fewer accounts with your real cell number, the smaller your SIM swap blast radius.

4. Carrier alerts

Most carriers offer SMS alerts when account changes happen. Enable these.

If your number gets ported out, you'll get a brief warning before service drops. That window may be enough to call the carrier and reverse it.

5. Don't broadcast your carrier

Doxers and SIM swap attackers can sometimes find your carrier from your number prefix or breached data. They use this to know which carrier to call.

Don't post your real number publicly. Don't put it on your business card, your website, your social media bio. Use a VoIP number for public-facing communication.

The eSIM social engineering threat

A newer attack vector: eSIMs can be issued instantly via QR code. An attacker doesn't need to wait for a SIM to ship. They social-engineer the call center, get an eSIM QR code, scan it into their device, and they have your number in minutes.

Defense: same as above (number lock, get off SMS 2FA), plus a habit of monitoring your cell service. If you suddenly lose all bars or "no service" appears unexpectedly, treat it as a potential SIM swap in progress.

What to do if you suspect a SIM swap

1. Call your carrier from another phone immediately. Ask if any port-out, SIM change, or eSIM transfer has been initiated.
2. If yes, demand it be reversed and escalate to fraud department.
3. While that's happening, log into your most sensitive accounts from a computer and change passwords. Email first, then banking.
4. Check Find My to see if your phone is reporting in.
5. Contact your bank's fraud line proactively.
6. File an FBI IC3 report at ic3.gov.

The bottom line

The single most preventable, most damaging attack on consumer phones. Set the carrier lock. Get off SMS 2FA. Audit phone numbers on your accounts.

One Saturday afternoon. Prevents most of the financial damage that SIM swap victims report.

SECTION 19: ANONYMOUS CELLULAR AND DATA-ONLY eSIMS

For most users, the carrier you sign up with in your real name is fine if SIM swap defense is set up. For higher needs, the goal is to separate the cellular pipe from your identity entirely.

The concept

Your phone needs cellular service to make calls and use mobile data when you're away from Wi-Fi. But cellular service doesn't have to be in your real name, with your real address, on your real credit card.

This is harder than it was five years ago. Regulations have tightened. But paths still exist.

Path 1: Prepaid in alias name (lightest)

Walk into a prepaid carrier (Cricket, Metro by T-Mobile, Boost) with cash. Sign up under an alias (legal use of a known nickname or middle name as first name is generally fine).

Pay with cash. Use a service address that isn't your home (UPS Store mailbox, registered agent address if you have an LLC).

You now have cellular service. The carrier knows the SIM is active and what tower it connects to, but they don't know your real name, real address, or your other accounts.

Path 2: LLC service (clean)

If you have an LLC, sign up for business cellular service in the LLC's name. T-Mobile for Business, Verizon Business, AT&T; Business all allow this.

The carrier knows the service is to an LLC. The LLC may or may not have your name as a member (Wyoming, Nevada, Delaware, and New Mexico keep LLC membership private). The bill comes to the LLC.

Cleanest path for business owners.

Path 3: Data-only eSIM (the strongest setup)

The most private setup. You don't have a "phone number" in the traditional sense. You have a data connection.

Several providers offer data-only eSIMs that don't require identity verification:

- Airalo: prepaid eSIMs for various countries. No KYC for short plans.
- Holafly: international data-only eSIMs.
- aloSIM, Nomad, Saily: other data-only eSIM marketplaces.

Sign up with an email (Proton alias), pay with Privacy.com or crypto, install the eSIM, you have data.

You don't have a phone number from the carrier. You don't have voice service from the carrier. The carrier just sees a data connection.

For voice and SMS, use a VoIP number (Section 20) routed over data.

The tradeoff: you need data signal everywhere you want to be reachable.

Path 4: Privacy-respecting MVNOs

Some smaller carriers have more flexible signup processes. Mint Mobile, US Mobile, and others let you sign up online with minimal verification.

Cape is worth a closer look for this layer. They're a privacy-first MVNO that operates their own mobile core (most MVNOs just lease from the big three). That gives them the ability to do things normal carriers can't: they rotate your IMSI identifier daily to disrupt persistent tracking, they encrypt SMS and voicemail at the network level, they have built-in SIM swap protection, and every plan comes with two additional phone numbers built in (useful for compartmentalization without needing a separate VoIP setup). They don't collect or sell location data. Not truly anonymous, but a meaningful improvement over a major carrier.

eSIM compatibility

Modern Pixels and iPhones support eSIM. The Pixel 8 and later support multiple eSIMs simultaneously. The iPhone 14 and later in the U.S. are eSIM-only.

eSIMs can be swapped, deleted, or compartmentalized quickly. You can have a primary eSIM for one use case and a secondary for another.

The compartmentalization strategy

For high-needs setups:

- Primary phone (GrapheneOS Pixel): data-only eSIM from Airalo or similar
- Voice/SMS: VoIP numbers from VoIP.ms, multiple numbers for different identities
- Real cell number (the carrier-assigned number): exists only as a backup data pipe, never given out

For everyday users:

- One carrier (preferably in LLC name or alias)
- One real cell number that's not given to anyone except family
- A VoIP number for everything else

Reality check

True anonymity at the cellular layer is hard. The carrier knows what tower you're using. Your phone's IMEI is recorded. Movements can be tracked at the network level.

What you're actually doing is decoupling cellular service from your identity. The carrier knows a SIM is active. They don't know it's you. That's a meaningful improvement over your real name on the account.

SECTION 20: PHONE NUMBERS AND VOIP

Your real cell number should be private. Not because it's secret (it isn't), but because it's the key to your SIM swap exposure and a lot of identity tracking.

What you actually want is multiple "phone numbers" for different purposes, none of which are your real cell number, all of which you control independently.

Why VoIP

VoIP (Voice over IP) numbers route through internet apps instead of cellular networks. You can have many. You can give different numbers to different parties. You can shut down a VoIP number that gets compromised without losing your other numbers.

VoIP is the foundation of phone number compartmentalization.

The provider: VoIP.ms

There are many VoIP providers. Twilio used to be popular but they changed their terms to be hostile to individuals. Google Voice works but Google has visibility into everything.

The standard recommendation is VoIP.ms. Canadian company. Years of reliable operation. Reasonable pricing. Supports SMS, MMS, and voice. Privacy posture is acceptable.

How it works:

1. Sign up at voip.ms with an email (Proton alias) and pay (Privacy.com card works, or crypto).
2. Add credit to your account ($25 minimum gets you a long way).
3. Order phone numbers (DIDs). About a dollar a month per number. Numbers available in most U.S. and Canadian area codes.
4. Configure each number's routing.
5. Use the VoIP.ms SMS app (iOS, Android, web) or a SIP client like Groundwire (iOS), Sipnetic (Android) for calls and texts.

Multiple numbers for multiple purposes

The whole point is compartmentalization. Get multiple numbers:

- Public number: business cards, website, LinkedIn. People email you, this is the number you give. If it ends up on data broker sites, shut it down without affecting anything else.
- Banking number: bank, brokerage, accountant. Only financial institutions know it. If it's ever compromised, you know exactly where the leak was.
- Family number: friends and family. Long-term stable.
- Travel/services number: airlines, hotels, retail signups.
- Burner numbers: short-term use. Sign up for something, use this number, throw it away later.

Some users run ten or more VoIP numbers. Manage them in the VoIP.ms portal.

SIM swap immunity

A VoIP number is not subject to SIM swaps. Not tied to a cellular carrier. An attacker can't call up a carrier and have it transferred.

This is why moving phone-number-dependent accounts (banking, email, crypto) to a VoIP number kills the SIM swap attack vector entirely.

Setup: change your bank's phone number on file from your cell to a banking VoIP number. Now even if someone SIM-swaps your cell number, your bank's phone-based recovery doesn't reach them. It still reaches you.

Practical limitations

Some services refuse VoIP numbers for verification. Banks, especially. Government agencies, often. They use phone validation services that detect VoIP and reject it.

When this happens:

- Use a "premium" VoIP service not detected as VoIP (some providers offer this).
- Use a prepaid cell number for the specific service that refuses VoIP.
- Push back: tell them you don't have a cell number and need a workaround.

For most services, VoIP works fine.

E911 and emergency services

A real cell number can be located via E911 if you call 911. A VoIP number's location depends on what you configured.

For most VoIP providers, you set a registered address that 911 calls route to. If you need to call 911, this should be accurate.

Keep your real cell number active for emergencies. Use VoIP numbers for everything else.

SIP clients

iOS: Acrobits Groundwire is the standard. $9.99 one-time. Configure with your VoIP.ms credentials.

GrapheneOS / Android: Sipnetic. Free.

For SMS, use the VoIP.ms web portal or their dedicated SMS apps.

The bottom line

If you're doing serious phone privacy work, VoIP isn't optional. Your real cell number being the credential for your bank, your email, your crypto, your social media is the single biggest exposure most people have.

Get a VoIP.ms account. Get four or five numbers. Move accounts off your real cell systematically. Within a month, your real cell number serves as nothing but a data pipe and your family contact.

PART 6 — PHYSICAL AND SITUATIONAL

SECTION 21: FARADAY BAGS

A Faraday bag is a pouch lined with conductive material that blocks all radio signals. Put your phone in one and it can't transmit or receive anything. No cellular. No Wi-Fi. No Bluetooth. No GPS. No NFC.

The cage was invented in the 1830s. The bags are cheap. They work.

When to use one

Sensitive meetings: when you're in a confidential conversation and you want zero chance of a phone being a recording device, in the bag.

Storage: if you're not using a sensitive phone for a while, store it in a Faraday bag.

Doctor/therapist/lawyer visits: some professionals require phones in Faraday bags or lock boxes during sessions.

When you want to go "off grid" briefly: walking, dinner with family, time without notifications.

Why "off" isn't enough

A phone that's "off" isn't fully off. Modern phones have a residual power state that lets them respond to Find My pings, run scheduled tasks, and in some forensic scenarios, be compromised.

Airplane mode disables most radios but isn't a hardware-level guarantee. A compromised phone could lie about being in airplane mode.

A Faraday bag is a hardware-level guarantee. Physics doesn't care what the OS is running.

Buying one

Quality matters. Cheap "Faraday" pouches from Amazon often leak signal. Test before relying on it.

Recommended brands:

- Mission Darkness
- SLNT (formerly Silent Pocket)
- EDEC (forensic-grade)

Cost: $30-100 depending on size and quality.

Testing your bag

Before you trust it:

1. Put your phone in the bag, fully closed.

2. From another phone, call your bagged phone.
3. The bagged phone should not ring or vibrate. Voicemail should pick up on the other end.
4. From the bagged phone (without opening), attempt to GPS-locate it via Find My.
5. The phone should not appear, or should show a "last seen" timestamp from before the bag.

If either test fails, the bag isn't blocking signals adequately. Return it.

Test periodically. A bag can degrade with use.

Faraday bags don't make you invisible

The bag blocks signals while the phone is inside. It doesn't:

- Prevent the carrier from logging your last known location before the phone entered the bag
- Hide what you do on the phone before or after using the bag
- Erase data already on the phone
- Provide forensic protection if the phone is taken and removed from the bag

Use the bag for tactical situations, not as a substitute for the rest of your privacy work.

SECTION 22: THE COMBINED SETUP

The combined setup: iPhone for daily life and the Apple ecosystem, GrapheneOS Pixel for sensitive activity. This is the strongest setup short of going GrapheneOS-only.

Why two phones

Different activities have different needs. Treating them all on one device means everything gets the security of the lowest-trust app on that device.

Your banking app needs to work. Some banks require Apple's ecosystem. Your family communicates on iMessage. Your business calendar is in Apple's ecosystem. Apple Watch needs an iPhone.

But you also have activities that need maximum privacy: anonymous communications, sensitive accounts not tied to your real identity, communications with specific high-trust contacts, work that needs full compartmentalization.

One device can't do both well. Two devices, each optimized for its job, can.

The split

iPhone:

- Personal/family identity
- Apple ID under your real or near-real identity
- iMessage for family

- Banking apps
- Apple Pay
- Apple Watch
- Non-sensitive photos
- Calendars and contacts you want synced across devices
- Your "public" identity

GrapheneOS Pixel:

- Anonymous identity
- Signal for sensitive contacts (separate Signal account with a different phone number)
- VoIP.ms calls and SMS for any number that's not your "public" identity
- Sensitive notes (Standard Notes, Joplin)
- Sensitive photos
- Sensitive browsing
- Cryptocurrency wallets
- Anonymous email accounts (separate Proton account from your daily one)
- Work requiring compartmentalization

Two cellular accounts

iPhone: regular postpaid or prepaid in your name or LLC. Your "known" phone.

GrapheneOS Pixel: data-only eSIM from an anonymous source (Airalo, Holafly). No identity tied to the cellular layer. Voice and SMS via VoIP numbers routed over data.

The two phones don't typically know about each other from the carrier's perspective.

Two phone number setups

iPhone: your "known" cell number. Family has it.

GrapheneOS Pixel: never uses a real cell number. All voice and SMS via VoIP numbers.

Daily usage pattern

iPhone constantly. Pixel for specific activities.

Morning: iPhone for everything normal. Check news, family iMessage, business calendar, photos.

When you have sensitive work: switch to the Pixel. Open the relevant Signal account. Make calls via VoIP. Access sensitive accounts.

End of day: Pixel goes in a Faraday bag overnight if your situation warrants it.

Mental model

The iPhone is your "civilian" identity. Connected to your real life. Tracks normally.

The Pixel is your "operational" identity. Disconnected from the iPhone. No shared accounts. No shared cloud storage. No shared contacts.

When you cross between the two, do it deliberately. Don't sync contacts between them. Keep them logically separate.

Costs

Two devices: $500-1500.

Two cellular plans: $30-80/month combined.

Time to set up: a long Saturday for the Pixel side, including GrapheneOS install and configuration. Less for the iPhone.

Not cheap. For the needs it serves, it's the right answer.

Alternative: iPhone primary, occasional Pixel use

If you don't need the full operational identity:

iPhone is your daily driver per Part 3.

Keep a GrapheneOS Pixel at home in a drawer. Use it for occasional sensitive web browsing, anonymous account access, communication with specific contacts.

The "weekend phone" approach. Less work, less ongoing cost. Still gets you most of the benefit.

One of the harder configurations to get right yourself. One of the highest-impact privacy upgrades available.

If you want one of these phones already configured, fully private, done for you, ready to use with instructions for anything regarding the phone, DM @truce_privacy.

PART 7 — MAINTENANCE

SECTION 23: THE QUARTERLY PHONE AUDIT

Privacy decays. Settings reset on OS updates. Permissions creep back. Apps update with new defaults. New apps you install grant themselves permissions you didn't intend.

Without maintenance, the work you did setting up your phone slowly erodes.

Run this audit every three months. Put it on your calendar.

iPhone quarterly audit

OS updates: Settings > General > Software Update. Install pending updates.

App updates: same. Outdated apps have unpatched vulnerabilities.

App inventory: open the App Library. Scroll through every installed app. If you haven't opened it in a month, delete it. Apps you don't use are pure attack surface.

Permissions sweep: Settings > Privacy & Security. Click into each category. For each app listed, ask: does this app still need this permission? Revoke anything that doesn't.

Special attention to Location Services > System Services. New iOS versions sometimes add new system services with default permissions. Audit each one.

Significant Locations: Settings > Privacy & Security > Location Services > System Services > Significant Locations > clear history.

Apple ID review: Settings > [your name] > Sign-In & Security. Check connected devices. Anything you don't recognize? Remove it.

Subscriptions: cancel ones you don't use.

Storage review: Settings > General > iPhone Storage. Look at what apps are taking space.

Safari history: Settings > Safari > Clear History and Website Data.

Backup verification: is iCloud Backup still on? Is ADP still on?

Stolen Device Protection: still on? Still set to Always?

Test Find My: from another device or icloud.com, confirm you can locate your iPhone.

Time required: 30-60 minutes per quarter.

GrapheneOS quarterly audit

OS updates: GrapheneOS pushes updates frequently. Settings > System > Advanced > System update. Should be set to automatic.

App updates: open the GrapheneOS App Store, Aurora Store, F-Droid, and Sandboxed Google Play (if installed). Update everything.

App inventory: review installed apps per profile. Uninstall what you don't use.

Permissions sweep: Settings > Privacy > Permission Manager. Review each permission category. Pay extra attention to:

- Network (the INTERNET permission you have unique control over). Revoke for apps that don't need it.
- Sensors. Revoke for apps that don't need it.
- Location. Approximate vs precise. Aggressively limit precise.
- Microphone. Time-limited grants where possible.

Profile review: are your profiles still organized the way you want? Any apps that should move between profiles?

Network: are you still using your intended VPN?

Backup: are you backing up to where you intended?

Duress PIN: is it still set? Do you still remember which is which?

USB-C settings: still on "charging-only when locked"?

Auto-reboot setting: still appropriate?

Sandboxed Google Play: in the right profile only? Not active in your sensitive profile?

Time required: 45-90 minutes per quarter.

Both platforms: the cellular layer

VoIP.ms account: log in. Verify your numbers are still active. Check for any unusual activity.

Carrier account: log in. Verify your number lock is still set. Check recent account activity for unauthorized changes.

Phone numbers on accounts: every six months, sweep "which accounts have my real cell number on file." Move new ones to VoIP.

The reboot habit

Reboot your phone weekly. Puts it in BFU state. The BFU state is harder for forensic tools to extract data from than the AFU state.

Easy way: reboot every Sunday night.

Why this matters

The single biggest reason people fall out of good privacy hygiene isn't laziness. It's lack of a maintenance habit.

The phone you set up perfectly in January is leaking data again by July if you never touch the settings. iOS updates add new features that default on. Apps update with new analytics SDKs. Permission requests get re-prompted and you tap through them without thinking.

The audit forces you to look at it. Forces you to notice the drift. Forces you to fix it.

Sixty minutes every three months. Put it on the calendar. Don't skip it.

SECTION 24: QUICK-START CHECKLIST

If you're not going to read the whole guide cover to cover, this is the minimum you should hit. Three to four hours of work this weekend.

iPhone

1. Update to the latest iOS version.

2. Change passcode to a 12+ character alphanumeric passphrase. Settings > Face ID & Passcode > Change Passcode > Custom Alphanumeric.

3. Enable Advanced Data Protection. Settings > [your name] > iCloud > Advanced Data Protection. Set up recovery contact and recovery key first.

4. Set Stolen Device Protection to Always. Settings > Face ID & Passcode > Stolen Device Protection > On > Require Security Delay > Always.

5. Turn off Analytics & Improvements. Settings > Privacy & Security > Analytics & Improvements > all toggles off.

6. Turn off Personalized Ads. Settings > Privacy & Security > Apple Advertising > Personalized Ads off.

7. Disable App Tracking globally. Settings > Privacy & Security > Tracking > Allow Apps to Request to Track off.

8. Audit Location Services. Settings > Privacy & Security > Location Services. Set most apps to Never or While Using. System Services > turn off Significant Locations, iPhone Analytics, Routing & Traffic.

9. Enable Mail Privacy Protection. Settings > Mail > Privacy Protection > Protect Mail Activity on.

10. Set Safari to use a privacy search engine. Settings > Safari > Search Engine > DuckDuckGo or Brave Search.

11. Set up Private Wi-Fi Address on each network you connect to.

12. Call your carrier and set up a port-out PIN.

13. Switch 2FA on your most important accounts (email, banking) from SMS to authenticator app or hardware security key.

14. Set up a VoIP.ms account. Get at least one number for non-essential signups.

15. Schedule a quarterly audit.

GrapheneOS

If you're going the GrapheneOS path:

1. Buy a supported Pixel (9a or 10a recommended) per Section 12.

2. Install GrapheneOS per Section 13. Lock the bootloader after installation.

3. Set a strong alphanumeric passcode (12+ characters).

4. Configure your profile setup per Section 14. At minimum, separate Owner from a Daily profile.

5. Set up Sandboxed Google Play in a dedicated profile if you need apps that require it.

6. Go through your installed apps and revoke INTERNET permission for any that don't need it.

7. Configure Auto-reboot (Settings > Security > Auto reboot) to a setting that fits your needs.

8. Verify USB-C is set to "charging-only when locked."

9. Decide whether to configure a Duress PIN. If yes, set it carefully.

10. Set up VoIP.ms account and numbers for voice and SMS.

11. Get a data-only eSIM if you want to separate cellular from your identity.

12. Schedule a quarterly audit.

Both platforms: the SIM swap layer

1. Set carrier number lock / port-out PIN.

2. Move banking, email, crypto, and social media 2FA off SMS to hardware key or authenticator app.

3. Audit accounts for which ones have your real cell number. Replace with VoIP where possible.

4. Get hardware security keys (YubiKey 5C NFC works with both iPhone and Pixel).

That's the minimum. Do this weekend.

CLOSING NOTES

Your phone is the single highest-leverage privacy investment you can make. Eighteen hours a day, on you, broadcasting your location, your communications, your identity.

You've now read the most thorough phone privacy guide I know how to write. iPhone hardening end to end. GrapheneOS as the strongest option. The cellular layer most guides skip. The physical and situational considerations that matter. The maintenance habit that keeps everything from drifting.

Most people don't do this work. They read about privacy, think about doing it, and never actually change their settings. Then they get SIM swapped, or doxed, or their location data appears in an embarrassing context, and they wish they had.

Don't be that person. Run the quick-start checklist. Do the work this weekend.

Your phone is the whole game. Lock it down.