How to Set Up a Phone That Can’t Be Tracked:
A Step-by-Step Guide

Building an Anonymous Phone: The Big Picture

This guide offers practical, easy-to-follow strategies for creating a privacy-focused phone while staying informed about potential risks. It’s designed to help you take control of your personal information, making your digital communications harder to trace while balancing ease of use and security.

At its core, the approach is all about **blending in while staying private**. By mimicking everyday behaviors—like buying in high-traffic locations or using mid-range devices—you make it harder for anyone to pick you out of the crowd. While achieving perfect privacy isn’t possible, the goal is to make it difficult and resource-intensive for anyone trying to track you.

Below is an extremely detailed Guide of everything you should do to create and maintain an untrackable phone. It is a LOT of information and steps.

For an abbreviated version that gets you most of the way there, see our Quick Steps version.

Quick Steps to an Untrackable Phone

Cheatsheet for Staying Anonymous

The process centers on a **layered approach** to anonymity. Think of it as building a fortress—each layer adds another barrier, making it harder for someone to break through. Here's how it works:

- **Keep Your Identity Separate**
  Avoid linking any part of your setup (like your SIM card, accounts, or payments) to your real identity. Cash and prepaid options are your best friends here.
- **Choose Untraceable Tools**
  Select phones and SIM cards that don't have ties to you. Older or mid-range devices are better since they're less likely to have unique tracking features.
- **Protect Your Data**
  Use secure apps like Signal and privacy-focused operating systems like GrapheneOS. A good VPN and temporary phone numbers add even more protection by hiding your activity.
- **Minimize Your Digital Footprint**
  Stay off home or work networks and avoid public Wi-Fi that's tied to you. Prepaid mobile data is safer for your online activity.
- **Tighten Your Tools**
  Turn off features that could leak information, like Bluetooth or GPS. Stick to privacy-first apps and browsers, like Tor or Brave, for what you really need.
- **Be Smart About How You Use It**
  Keep your anonymous phone and activities separate from your regular life. For example, don't log into your personal accounts or connect to familiar networks.
- **Refresh Regularly**
  Start fresh by wiping and resetting your phone every so often. If you're serious about privacy, tools like Faraday bags can block signals entirely when your phone isn't in use.
- **Think Beyond the Device**
  Physical habits matter, too. Avoid stores or places where you're easily recognized, and change up how and where you make purchases to keep patterns unpredictable.

By following these principles, you'll build a phone setup that's tailored for privacy. Whether you're new to the idea or an experienced privacy advocate, this guide equips you to stay ahead of the game and make your digital life as anonymous as possible. Ready to get started? Let's dive in:

5 Steps to Set Up a Phone That Can't Be Tracked

⭕ Step 1: Buy SIM Card & Gift Card

Buying a SIM card with cash and activating it anonymously are key steps to prevent anyone from tying the phone to your real identity or location.

App stores require a payment method to set up an account. By using a prepaid gift card bought with cash, you avoid entering personal credit card or bank details, keeping your identity out of the system.

Get Cash	Buy SIM	Buy Gift Card

1. Obtain Cash

- Use any method to get cash. You're going to need at least $50 for service activation. You may need more if you are purchasing a used device with cash.
    - Cashback from grocery stores or retailers.
    - ATM withdrawals.
    - Cash from paycheck-cashing services.
- The cash doesn't need to be anonymous. The key is to ensure no connection between the cash source and the SIM purchase we are going to make.

2. Buy a Prepaid SIM Card

- Visit large chain stores like **Target**, **Walmart**, **Best Buy**, drugstores, or convenience stores.
- Select a prepaid SIM card from carriers that don't require personal details for activation. Some good options include:

    - ⭐ **Mint Mobile**: Affordable and easy activation with minimal data required.
    - ⭐ **Tracfone**: Available widely; does not require an ID for setup.
    - **AT&T Prepaid**: Offers prepaid SIMs with minimal registration requirements.
    - **Tello**: Operates on the T-Mobile network, offering flexible prepaid plans.
    - **Lycamobile**: International focus; no ID required for setup.
    - **H2O Wireless**: Prepaid SIMs with anonymous activation available.

- Pay with cash to avoid linking the purchase to your identity.

3. Purchase a Gift Card

- Obtain an **Apple Store** **or** **Google Play gift card** with cash.

- Use this gift card later to set up an Apple ID or Google Play account without providing a credit card or personal details.
- If you want to purchase other types of gift cards to enhance privacy of transactions, see >> **ObscureIQ's Guide to Prepaid Cards**

Key Tips

- If the store logs or scans SIM purchases, prioritize buying in high-traffic, anonymous locations to blend in.
- Avoid purchasing from stores where you're known or that might keep transaction data tied to your identity.
- If someone was really trying hard to find you they might connect the Card or SIM number to the purchase at the store. They could then look at videotape to see who made the purchase.

⭕ Step 2: Buy & Wipe a Phone

The point of sourcing a clean phone and thoroughly resetting it is to ensure there are no ties between the device and your personal identity, and to eliminate any lingering data or software that could compromise your privacy.

A used or refurbished phone that hasn't been fully wiped might still contain traces of its previous owner's accounts, data, or even spyware.

Get a Phone	Factory Reset	Reformat

1. Source a Phone

- When obtaining a phone for off-grid use, the goal is to ensure it has no ties to your personal identity or prior usage.

- See the full guide the **Sourcing** here:

  >> **ObscureIQ's How to Buy a Used Phone for Privacy**.

  Below is an abbreviated guide.

- **Option 1: Purchase a Used Phone with Cash**
  - Where to Buy:
    - Local Pawn Shops, flea markets, electronics resellers, or classified ads Also try to connect with sellers via **Craigslist** or **Facebook Marketplace**.
- **Option 2: Purchase a Refurbished Phone Online Anonymously**
  - Where to Buy:
    - Use platforms like **Swappa**, **Decluttr**, or **Back Market**.

- **Option 3: Use an Old Phone You Already Own**
  - Ensure No Personal Connections:
    - Remove any previously linked Apple/ Google accounts or SIM cards.

2. Factory Reset the Phone

- Erase all existing data by performing a factory reset.
- Ensure there is no pre-installed SIM card.

3. Reformat the Phone

- Put the phone in recovery mode and connect it to a computer with no linked Apple or Google accounts.
- Reformat the phone to ensure a clean slate.

⭕ Step 3: Set Up Accounts & Activate Phone

Using public Wi-Fi to set up a VPN before activating your anonymous phone is crucial because it prevents any direct connection between your device and a location or network that could identify you. This ensures your phone's setup is as untraceable as possible.

Public Wi-Fi	MullVad VPN	Create Email
OS Account	Activate SIM	Strong Code

1. Find Public Wi-Fi

- Use Wi-Fi at a library, café, or public space that is not linked to you.
- Choose a location you rarely visit or never plan to return to.
- **Do not use your home or work Wi-Fi.**

2. Set Up Mullvad VPN

To maximize anonymity, start by creating a free **Mullvad** VPN account. Mullvad is unique because it doesn't require an email address, allowing you to set up a VPN without compromising privacy. **Mullvad** doesn't require an email, making it ideal for anonymity.

- Access Mullvad's website and click Generate Account.
  - Mullvad will create a random account number for you.
  - Write it down securely.
- Download and activate the Mullvad VPN app on your phone.
- Choose a VPN server unrelated to your current location.

3. Create a Disposable Email

With Mullvad active, use a secure, privacy-focused email provider to create an account without requiring personal information. Recommended options:

- ⭐ **Proton Mail**: Highly secure, offers anonymous sign-ups, and doesn't require a phone number.
- ⭐ **Tutanota**: End-to-end encryption with anonymous account creation and optional paid plans for expanded storage.
- **Guerrilla Mail**: Temporary, disposable email addresses with no sign-up required (good for one-time use).
- **SimpleLogin**: Generate aliases to protect your real email while forwarding messages to your inbox.
- **AnonAddy**: Similar to SimpleLogin, creates disposable email aliases for privacy.

Tips for Maximum Anonymity:

- Use non-identifiable information (e.g., random usernames) during sign-up. Avoid anything that can be tied back to you.
- Do not link this email to any existing personal accounts. No email forwarding. That's inconvenient but important.

4. Set Up Your Apple or Google Account

- Use the gift card you purchased to create an Apple ID or Google account.
- Input a random billing address if prompted.

5. Activate the SIM Card

- Insert the prepaid SIM card into the phone and activate it using the public Wi-Fi.
- Avoid entering any personal information.

6. Secure the Phone

- Set a strong six-digit security code (avoid common combinations like 123456).
- Disable Face ID or Touch ID features.

⭕ Step 4: Ready Your Phone for Use

Bluetooth Off	VPN On
Install Apps (necessary only, no personal data)	
Private Browsing	Encrypted Messaging
Disable Cloud Services	

Privacy Settings (Apple)	Privacy Settings (Android)
Mask Phone Number	Block Caller ID
Turn off Wi-Fi (use phone data plan)	

1. Disable Bluetooth

- Turn off Bluetooth to prevent third-party tracking or data interception.

2. VPN

- Ensure the VPN is always active when using the phone.
- Mullvad is a great option, but alternatives like ProtonVPN or NordVPN work too (ensure anonymity during registration).

3. Install Apps

- **Only** download necessary apps using the VPN to mask your activity.
- **Do not** give apps your personal information, or login to existing accounts. This will compromise you, allow them to tie your anonymous phone to your existing profiles.

* Get a Private Browser

- Replace the default browser with **Tor Browser** or **Brave** or **Duck Duck Go** for better privacy.
- **Do not use Chrome**

* Get Encrypted Messaging

- Install secure apps like **Signal** for private, end-to-end encrypted communication.
- Avoid linking these apps to personal accounts or phone numbers.

* Disable Cloud Services

- Disable cloud backups for apps like **Google Drive**, **Google Keep**, **Google Photos**.
- Go to `Settings → Apple ID → iCloud → Apps` Using **iCloud** and turn off unnecessary features.
- If you want secure Cloud services, use something like
  - **Proton Drive**: Use a ProtonMail account created with a disposable email and connect via a VPN for added anonymity.
  - **Tresorit**: Use a pseudonym and a prepaid gift card for account creation and payment.

Mask Your Phone Number

- Use temporary number services like Hushed or Silent Phone for calls and texts.

Block Caller ID

- Disable outbound caller ID in your phone's settings or use prefix codes like *67 (U.S.) before dialing.

* Privacy Settings for iPhone Users

- **Turn Off Significant Locations:**
  - Navigate to: `Settings → Privacy → Location Services → System Services → Significant Locations`.
  - Disable Significant Locations to prevent Apple from logging your frequently visited places.
- **Limit App Permissions:**
  - Go to: `Settings → Privacy → Location Services`.
  - Review app permissions and restrict access to only those that are essential. Use "While Using the App" or "Never" for location access whenever possible.
- **Disable Analytics and Diagnostics:**
  - Navigate to: `Settings → Privacy & Security → Analytics & Improvements`.
  - Turn off all options, including "Share iPhone Analytics" and "Improve Siri & Dictation," to stop Apple from collecting usage data.

* Privacy Settings for Android Users:

1. **Turn Off Location Services:**
   - Navigate to: `Settings → Location`.
   - Disable location services entirely, or selectively adjust app permissions to "Deny" or "Only While Using the App."
2. **Disable Background Location Tracking:**
   - Go to: `Settings → Apps → [App Name] → Permissions → Location`.
   - Ensure no app has unrestricted access to your location in the background.
3. **Limit App Permissions:**
   - Navigate to: `Settings → Privacy → Permission Manager`.
   - Review app permissions and deny access to features like camera, microphone, or location unless strictly necessary.
4. **Disable Analytics and Diagnostics:**
   - Navigate to: `Settings → Privacy → Usage & Diagnostics`.
   - Toggle off any options related to sharing diagnostic or usage data with Google or other parties.

* Turn Off Wi-Fi After Setup

- Avoid using Wi-Fi after the initial setup. Use the phone's data plan instead.

⭕ Step 5: Maintain Anonymity

Tips for keeping your anonymity when using your phone. Getting it set up right is crucial, but you can do things that compromise that privacy if you are not careful.

Use Cash	Mobile data	Forget Wi-Fi
Isolate	Limit use	VPN Switch
Avoid Behavioral Patterns		

Use Cash for Payments

- Pay for additional SIM card data or phone services with gift cards purchased using cash. Avoid auto-renewal Wi-Fi.

Prioritize Mobile Data

- Avoid Wi-Fi whenever possible. Rely on prepaid data plans for all online activities.

Forget Wi-Fi Networks

- After using public Wi-Fi, If you have to use one, go to Network Settings and “forget” the network to remove the digital trail.

Avoid Home Wi-Fi

- **Never** connect the phone to your personal home network.

Isolate Device Use

- If traveling with both a personal and anonymous phone, **do not connect both to the same Wi-Fi network simultaneously**.
- Power off your anonymous phone when not in use.

Limit Usage

- Use the phone only for its intended purpose. Avoid casual browsing or app installations beyond essentials.

Use a VPN and set up a Kill Switch

- Ensure the VPN is active and functioning correctly during use.
- You can set up a **kill switch** in most VPNs. The kill switch will turn off your internet access if your VPN is disabled. This will keep you from accessing the internet without the protection of your VPN.
- Periodically recheck VPN settings to maintain security.

Avoid Behavioral Patterns That Could Expose You

Even with a highly secure phone, consistent behaviors can create vulnerabilities. Adversaries might track your physical movements or habits to link your activities to your identity. Here's how to stay unpredictable:

- Vary the Locations Where You Use Public Wi-Fi
  - If you always connect to Wi-Fi at the same coffee shop, someone monitoring the network or reviewing surveillance footage could identify you. Instead, rotate between different public Wi-Fi spots, like libraries, malls, or parks, and avoid using Wi-Fi at locations you frequent for personal reasons.
- Avoid Routine Purchases at the Same Stores
  - Regularly buying gift cards or prepaid SIMs at the same retailer could create a pattern that links you to these purchases. Spread your purchases across different stores and choose high-traffic times to blend in with crowds.
- Change Travel Routes
  - If you often visit the same places with your anonymous phone, like a certain grocery store or public space, someone could track your movements. Switch up your routes and destinations to make tracking harder.
- Power Off the Device in Familiar Locations
  - If you bring your anonymous phone to your workplace or home, its signal could betray your identity. Power off the phone before entering these areas, or better yet, don't take it there at all.
- Mix Up Activity Patterns
  - If you always activate your VPN or check your anonymous email at the same time of day, it could create a detectable pattern. Use these services at different times to avoid predictable behavior.
- Limit Physical Proximity to Personal Devices
  - If you carry your anonymous phone and personal phone together, Bluetooth or Wi-Fi signals could reveal that both devices are used by the same person. Keep your anonymous phone physically separate and avoid connecting them to the same networks.

⭕ Advanced Tricks

Onions	Private DNS	Custom OS

1. Use Onion Routing

- Use Tor over VPN for an additional layer of anonymity when accessing the internet.

2. Deploy Secure DNS Settings

- Secure DNS prevents ISPs, attackers, or other intermediaries from tracking the websites you visit. It mitigates threats like DNS spoofing or cache poisoning, which can redirect users to malicious websites. Secure DNS encrypts and protects internet activity, ensuring greater privacy and security online. Free services are ok, but paid services are safer.
    - **Control D** (premium)
    - **NextDNS** (premium)
    - **Quad9** (non-profit)
    - **Cloudflare 1.1.1.1**, **Google Public DNS** (free)

3. Install Security-Focused Operating Systems (for Android users)

- Replace the stock Android OS with privacy-focused alternatives like GrapheneOS or **CalyxOS**. These minimize tracking and data collection.

⭕ Managing Physical Privacy

Faraday Bag	Limit GPS	Don't Link

Prevent Physical Tracking

- Use a **Faraday bag** when the phone is not in use to block RF signals entirely.
- Always turn off GPS when not needed.
- Putting your phone into Airplane Mode can be an easy way to accomplish this.

Avoid Linking Accessories

- Do not connect wearables (e.g., smartwatches) or other Bluetooth accessories to the device. Remember, Bluetooth is bad because it allows location tracking.

⭕ Tips for Sustaining Anonymity Long-Term

Rotate Cards	Multiple Phones	Rewipe
Monitor Threats		
Have a Recovery Plan		

Rotate Gift Cards and SIM Cards

- Avoid frequenting the same retailer or using the same carrier to prevent pattern recognition.

Maintain Multiple Burner Phones

- Use separate devices for distinct tasks (e.g., one for messaging, another for browsing).

Regular Maintenance

- Periodically wipe and reformat the phone to remove traces of activity or potential malware.
- It sounds like a pain in the ass but starting over fresh 6 to 12 months is a good idea.

Stay Updated on Privacy Threats

- Follow blogs, forums, or newsletters from privacy advocates like the Electronic Frontier Foundation (EFF) to stay informed.
- Our TacticalPrivacyWire.com is a good place for original research and advice.

Emergency Recovery Plan

- Keep duplicate contact lists or important information in an encrypted backup.
- Be prepared to abandon the phone and set up a new one if it is compromised.

Disclaimer

The tools and services mentioned in this guide, such as Mullvad VPN and Proton Mail, are recommended based on their current reputation and features as of the time of writing. However, privacy-focused technologies, policies, and security practices can change over time. It is essential to independently verify the current status, terms of service, and effectiveness of any recommended tools or services before relying on them for anonymity or security. Always stay informed by consulting official websites, privacy advocate resources, or trusted reviews to ensure these solutions meet your needs and provide the expected level of privacy.