Here's your **complete mobile security setup** (tailored for activists, journalists, or high-risk users):

🔐 **1. Hardware Defense**

🧳 **Faraday Bag (for total RF isolation)**

- ✅ Blocks all signals (cellular, GPS, Wi-Fi, Bluetooth, NFC)
- 🔒 Use when traveling, attending sensitive meetings, or avoiding live tracking
- **Recommended Brands:** Silent Pocket, Mission Darkness

📱 **2. Secure Phone Options:**

. Use a Secure Phone Operating System

- **Consider a Privacy-Focused OS**: Phones running **Android** and **iOS** are both vulnerable to data collection by corporations. However, privacy-focused operating systems, like **GrapheneOS** (for Google Pixel devices) or **CalyxOS**, offer enhanced privacy features and better security.
- **Custom ROMs**: If you're tech-savvy, you can install a **custom ROM** like **LineageOS** or **/e/OS** for more control over the OS and fewer pre-installed apps (especially those tied to Google).

- **GrapheneOS** on a Pixel 6/7/8:
    - Hardened Android OS
    - Strips all Google spyware
    - No forced Google Play Services
    - Open-source, audit-ready
- **CalyxOS** (more user-friendly than GrapheneOS)
    - Ideal if you still want some app convenience with privacy

Buy a clean Pixel device (unlocked), flash GrapheneOS/CalyxOS, and never sign into Google.

□ 🛡️ 3. VPN: **Mullvad** (no email or name required, can pay with crypto or cash)

□ 🔐 4. Browser: **Tor Browser** or **Brave (with strict settings)**

□ 🧼 5. Cleaner: **Hypatia AV**, **SD Maid**, or built-in tools from GrapheneOS

Phone Messaging:

🥇 6. **Session**

- 📱 Available on Android & iOS
- ✅ No phone number, email, or ID required
- 🔒 Uses **decentralized** onion routing (like Tor)
- 💬 End-to-end encrypted (based on Signal protocol but with no metadata)
- 🌐 Operates on a **decentralized Oxen network** (Thiel & Musk have no control or stake)
- 🧠 Open-source & maintained by a privacy nonprofit

Why it's best for you: No servers controlled by Big Tech, no data harvesting, and no need to ever provide personal info. It's also *not hosted on AWS, Azure, or Google Cloud* — another plus for avoiding surveillance networks.

🛑 **Avoid These:**

- ❌ **Signal** – Great security but needs a phone number and reportedly stores some metadata now
- ❌ **Telegram** – Can hide your number, but the backend is centralized and may be vulnerable
- ❌ **X (formerly Twitter DMs)** – Elon Musk owns it
- ❌ **WhatsApp** – Owned by Meta; metadata accessible, phone number required
- ❌ **Messenger, IG- Worst one's**

7. Use Strong Authentication

- **Enable Two-Factor Authentication (2FA)**: Use 2FA on your accounts whenever possible. Apps like **Authy** or **Google Authenticator** can help, but **Yubikey** (a hardware key) offers the most secure option.
- **Biometric Protection**: Use fingerprint or facial recognition only if you trust the hardware and software behind it. These features can sometimes be bypassed or exploited, so use them cautiously.
- **Strong PIN/Password**: Make sure your phone's screen lock has a strong, unique PIN or passphrase.

8. Limit Data Collection

- **Minimize Permissions**: Go through your apps and revoke unnecessary permissions. For instance, prevent apps from accessing your camera, microphone, location, or contacts if they don't need those features.
- **Turn Off Location Tracking**: Keep location services off unless absolutely necessary. If you need them on, consider using a GPS spoofing app.
- **Use Privacy-Focused Apps**:
    - **ProtonMail** or **Tutanota** (for secure email)
    - **DuckDuckGo** or **Brave** (for private browsing)
    - **Wire** (for secure video calls)

9. Encrypt Your Data

- **Full Disk Encryption**: Modern phones come with encryption enabled by default (i.e., Android and iOS), which means your data is protected if your phone is lost or stolen. Ensure this feature is active, especially on Android.
- **Use Encrypted Storage for Sensitive Files**: Consider apps like **Bitwarden** (for passwords) or **Cryptomator** (for encrypted cloud storage) to protect sensitive information.

10. Reduce Tracking & Surveillance

- **Use a VPN**: This hides your IP address and encrypts internet traffic. Pick a VPN that doesn't log data, like **Mullvad**, **ProtonVPN**, or **IVPN**.
- **Block Ads & Trackers**: Use apps like **Blokada** or **AdGuard** to block trackers and ads, preventing data harvesting.
- **Limit Google Services**: If you want to avoid tracking by Google (who's closely connected to Musk's ventures like Tesla and SpaceX), use a **Google-free phone** (using a custom ROM like **/e/OS**) or minimize your reliance on Google services.

11. Be Mindful of Apps & Services

- **Install Only Trusted Apps**: Stick to well-reviewed, open-source apps from reputable sources like F-Droid for Android (which offers privacy-focused apps).

12. Regularly Update Your Phone

- **Keep Your OS and Apps Updated**: This is one of the most important steps to prevent attacks. Regular updates patch security vulnerabilities.
- **Use a Security-Focused Browser**: Apps like **Firefox** with privacy extensions (like **uBlock Origin** and **HTTPS Everywhere**) can give you extra protection while browsing.

13. Beware of Social Engineering and Phishing

- **Be Cautious of Links and Attachments**: Musk, or any other entity, may not need direct access to your phone—they could try to trick you into installing malicious apps or giving away sensitive info through phishing attempts.
- **Enable Anti-Phishing Protection**: Use apps like **1Password** or **Bitwarden** (which also manage your passwords securely) that offer anti-phishing features.

14. Secure Your Cloud Data

- **Use Encrypted Cloud Storage**: Avoid using Google Drive or iCloud for sensitive data. Use **Tresorit**, **ProtonDrive**, or **Sync.com**, which encrypt your data end-to-end.
- **Backup Regularly**: Make sure you're backing up important files, but always use encrypted backup solutions.

15. Turn Off Unnecessary Features

- **Disable Bluetooth, Wi-Fi, and NFC** when not in use to reduce exposure to potential vulnerabilities or hackers.
- **Airplane Mode**: If you don't need to be reachable or use the internet, putting your phone in Airplane Mode can help block remote access.