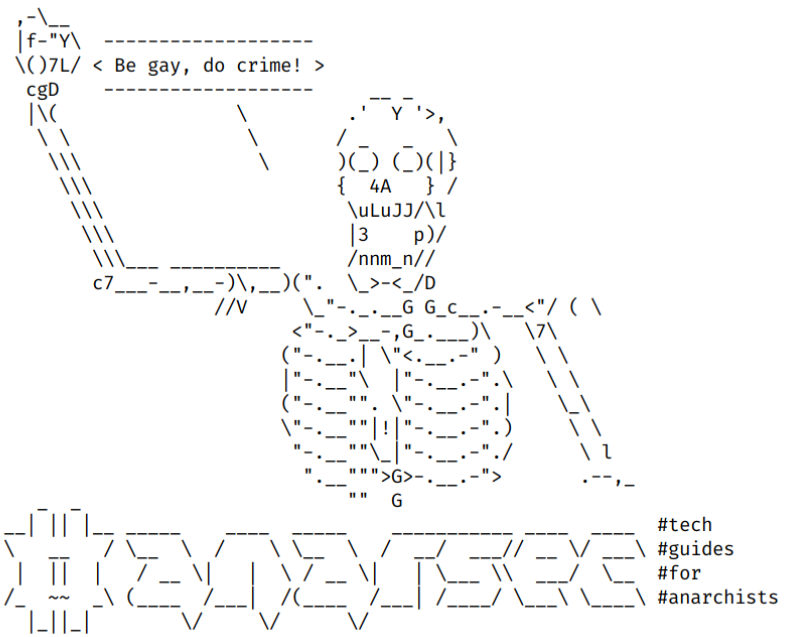
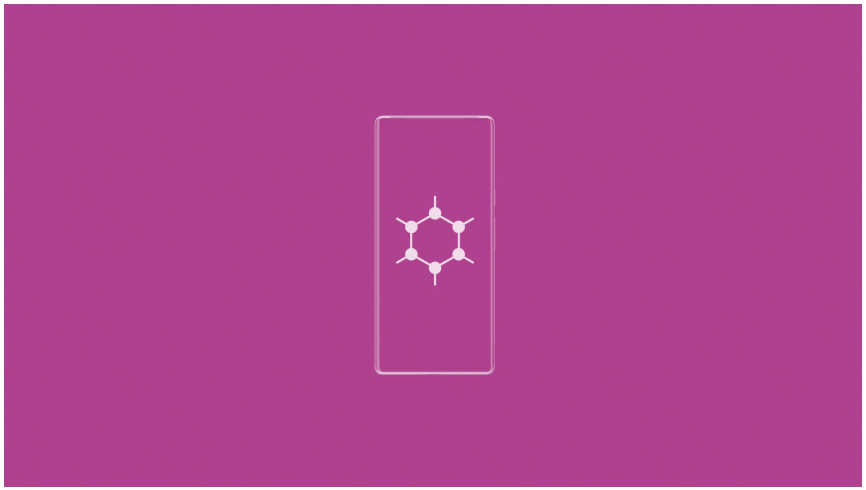
GrapheneOS for Anarchists

While anarchists should minimize the presence of phones in their lives, if you do decide to use a phone, make it as difficult as possible for an adversary to geotrack it, intercept its messages, or hack it. This means using GrapheneOS.





Series: Defensive

This version of the zine was last edited on 2024-04-22. Visit anarsec.guide to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for it. Ai ferri corti.

AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

Defensive

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Phones

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

General

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Offensive

Coming soon

Contents

It is important to emphasize this to cut through the widespread marketing hype; a VPN is not enough to keep you anonymous[103]. Using a VPN can be thought of as simply shifting your trust from a local Internet Service Provider which is guaranteed to be a snitch to a remote company that claims to limit its ability to effectively snitch on you.

For more information, see Privacy Guides[104], and for an excellent comparison of a VPN and Tor†, see Defend Dissent: Anonymous Routing[105].

[103] ivpn.net/privacy-guides/will-a-vpn-protect-me/
[104] privacyguides.org/en/basics/vpn-overview/
[105] open.oregonstate.education/defenddissent/chapter/anonymous-routing/

While anarchists should minimize the presence of phones in their lives[1], if you do decide to use a phone, make it as difficult as possible for an adversary to geotrack it, intercept its messages, or hack it. This means using GrapheneOS.

What is GrapheneOS?

GrapheneOS is a security-focused version of the Android operating system†. Standard Android smartphones have Google baked into them (for example, Google Play Services[2] has irrevocable access to your files, call logs, location, etc.). GrapheneOS removes all Google apps and services by default, uses hardware-based security to make it far more difficult[3] to bypass the disk encryption, and it is significantly hardened† against hacking. There are other alternative Android operating systems, but they don't have comparable security[4]. See the GrapheneOS documentation[5] for an extensive list of privacy and security improvements over standard Android.

Due to the nature of how the technology works[6], cell phones connecting to cell towers give the provider a history of your geolocation. For this reason, we recommend that you leave your smartphone at home and use it like a landline, connecting to the Internet via Wi-Fi in airplane mode, rather than using a SIM card to connect through cell towers. Even if you use an anonymously purchased SIM card, if it is linked to your identity in the future, the service provider can be retroactively queried for all geolocation data. Furthermore, it's not enough to only leave your phone at home when you're going to a demo or action, as this will stand out[7] as an outlier

[1] anarsec.guide/posts/nophones/
[2] en.wikipedia.org/wiki/Google_Play_Services
[3] grapheneos.org/faq#encryption
[4] eylenburg.github.io/android_comparison.htm
[5] grapheneos.org/features
[6] citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/
[7] anarsec.guide/posts/nophones/#metadata-patterns

and serve as an indication of conspiratorial activity in that time window.

Installation

Google Pixel[8] phones are currently the only devices that meet the hardware security requirements of GrapheneOS — see supported[9] and recommended devices[10]. "Hardware memory tagging support" is a very powerful security feature that was introduced with the Pixel 8, making it substantially harder to remotely exploit user installed apps such as Signal which has a "massive amount of remote attack surface"[11].

Starting with the Pixel 8, Pixel devices will receive at least 7 years of security updates from the date of release. End-of-life devices (GrapheneOS "extended support" devices) do not receive full security updates and therefore are not recommended. See how long GrapheneOS will support the device for[12].

Avoid carrier variants of the phone, i.e. don't buy one from a mobile operator, which may prevent you from installing GrapheneOS. The cheapest option is to buy the "a" model right after the next flagship model is released — for example, the Google Pixel 6a after the Pixel 7 is released.

GrapheneOS can be installed[13] using a web browser or the command line†. If you are uncomfortable with command line, the web browser installer is fine; as the instructions note[14], "Even if the computer you used to flash GrapheneOS was compromised and an attacker replaced GrapheneOS with their own malicious OS, it can be detected with

[8] privacyguides.org/android/#google-pixel
[9] grapheneos.org/faq#device-support
[10] grapheneos.org/faq#recommended-devices
[11] grapheneos.social/@GrapheneOS/111479318824446241
[12] grapheneos.org/faq#device-lifetime
[13] grapheneos.org/install/
[14] grapheneos.org/install/cli#verifying-installation

For more information, see Tails for Anarchists[100] and Privacy Guides[101]. To understand the limitations of Tor, see the Whonix documentation[102].

VoIP (Voice over Internet Protocol)

Google Voice is a well-known and insecure VoIP service; this technology routes your calls over the Internet (as Signal does) instead of using standard cell tower transmission. Unlike Signal, VoIP allows you to receive calls from anyone, not just other Signal users. The advantage of using VoIP for calls over a data plan is that you can create different numbers for different activities (one for bills, one for signing up for a Signal account, etc.), and you never need to turn off Airplane mode. The advantage of using a data plan instead is that you can use it away from Wi-Fi, at the cost of geolocation (i.e. it will be possible for your service provider and possibly other parties to know where your device is at any given time).

VPN (Virtual Private Network)

A VPN extends a private network (like your home network) over a public network (like the Internet). Devices connected to the VPN are part of the private network, even if they are physically located elsewhere. Applications that use a VPN are subject to the functionality, security, and management of the private network.

In other words, it is a technology that essentially makes it appear that you are connecting to the Internet from the network of the company providing the service, rather than from your home network. Your connection to the company is through an encrypted "tunnel". A VPN is not the best tool for anonymity (defined as knowing who you are — Tor is far better), but it can partially enhance your privacy (defined as knowing what you are doing).

[100] anarsec.guide/posts/tails/#tor
[101] privacyguides.org/en/advanced/tor-overview/
[102] whonix.org/wiki/Warning

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

Sandboxing

Sandboxing is the software-based isolation of applications to mitigate system failures or vulnerabilities. For example, if an attacker hacks an application that is "sandboxed", the attacker must escape the sandbox to hack the entire system. Virtualization[94] is the most powerful implementation of sandboxing.

Tor network

Tor[99] (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting". The Tor network can be accessed through the Tor Browser on any operating system. The Tails† operating system forces every program to use the Tor network when accessing the Internet.

[99] torproject.org/

Auditor", which is explained below. Both methods list the officially supported operating systems that you can install from.

The first time you boot Graphene, it will ask you if you want to connect to Wi-Fi. Don't, we need to do hardware-based attestation[15] first. Never set up fingerprint authentication. Set a strong password[16].

There is no official support for installing from Qubes OS, but it is possible with the following steps.

Installation on Qubes OS

These instructions assume that your sys-usb qube is disposable, which is the default in the post-installation settings[17], and that it uses a Debian template.

- In a disposable Whonix-Workstation qube, open the command line installation guide[18] using Tor Browser.
- You will read "Installing from an OS in a virtual machine is not recommended. USB passthrough is often not reliable." This means we will be doing everything from sys-usb, which does not use USB passthrough. If you set sys-usb to be disposable when you installed Qubes OS, it will be reset after a reboot.
- For simplicity, we will temporarily enable networking in sys-usb. It is also possible to keep sys-usb offline by copying platform-tools and the factory image from the disposable Whonix-Workstation qube into sys-usb, and getting udev rules from Github[19] instead of apt. In the **Settings → Basic** tab of sys-usb, make the following changes:
  - Private storage max size: 10.0 GB
  - Net qube: sys-firewall
  - Press **Apply**
- Follow the installation instructions in the sys-usb terminal. When you get to **Flashing factory images**, don't run `./flash-all.sh`. Instead, scroll down to Troubleshooting and run the command that

[15] anarsec.guide/posts/grapheneos/#auditor
[16] anarsec.guide/posts/tails-best/#passwords
[17] anarsec.guide/posts/qubes/#getting-started

uses a different temporary directory. The flash script is expected to print out messages like `archive does not contain 'example.img'`.
- When you're done, restart sys-usb. If it is disposable, the changes you made will be gone. Don't forget to change the sys-usb qube settings back:
  – Net qube: (none)

System navigation

GrapheneOS uses gesture navigation[20] by default. The essentials are:

- The bottom of the screen is a dedicated touch zone for system navigation.
- Swiping up from the navigation bar while removing your finger from the screen is the **Home** gesture.
- Swiping up from the navigation bar while keeping your finger on the screen before letting go is the **Recent Apps** gesture.
- Swiping from the left or right side of the screen within the app (not the navigation bar) is the **Back** gesture.
- The launcher uses a swipe-up gesture from anywhere on the screen to open the app drawer from the home screen. You must start this gesture above the system navigation bar.

Auditor

In the post-installation instructions, **Hardware-based attestation** is the last step. The Auditor app included in GrapheneOS uses hardware security features to monitor the integrity of the device's firmware and OS software. This is critical because it will alert you if these components of the device are maliciously tampered with. Note that Auditor doesn't necessarily check whether the user-level apps running

[18] grapheneos.org/install/cli
[19] github.com/M0Rf30/android-udev-rules
[20] grapheneos.org/usage#gesture-navigation

Exploit

An exploit is designed to take advantage of a vulnerability[94]. Even worse (or better, depending on whether you are the attacker or the target) are zero-day exploits[94].

Full Disk Encryption (FDE)

FDE means that the entire disk is encrypted[†] until a password is entered when the device is powered on. Not all FDE is created equal. For example, the quality of how FDE is implemented on a phone depends not only on your operating system, but also on your hardware (the model of your phone). FDE uses symmetric cryptography[94], and on Linux it typically uses the LUKS specification[94].

Hardening

Hardening is a general term for the process of securing systems against attacks.

Malware

Malware (malicious software) is a generic term for software that contains unwanted or malicious functionality. Malware includes ransomware, Trojan horses, computer viruses, worms, spyware, scareware, adware, etc. Today, malware is more difficult to categorize because sophisticated malware often combines characteristics of different categories. For example, WannaCry[98] spread like a worm, but encrypted files and held them for ransom (ransomware).

Open-source

The only software we can trust because the "source code" that it is written in is "open" for anyone to examine.

[98] en.wikipedia.org/wiki/WannaCry_ransomware_attack

Appendix: Glossary

Command Line Interface (CLI)

The "command line" is an all-text alternative to the graphical "point and click" tool that most of us are more familiar with; the Command Line Interface (CLI) allows us to do some things that a Graphical User Interface (GUI) does not. Often, either a GUI or a CLI would work, and which you use is a matter of preference. For example, in Tails†, you can verify the checksum[94] of a file using either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

For more information, see Linux Essentials[95]. The Tech Learning Collective's "Foundations: Linux Journey" course on the command line[96] is our recommended introduction to using the CLI/terminal.

Encryption

Encryption is the process of scrambling a message so that it can only be unscrambled (and read) by the intended parties. The method you use to scramble the original message, or *plaintext*, is called the *cipher* or *encryption protocol*. In almost all cases, the cipher is not intended to be kept secret. The scrambled, unreadable, encrypted message is called the ciphertext and can be safely shared. Most ciphers require an additional piece of information, called a *cryptographic key*, to encrypt and decrypt (scramble and unscramble) messages.

For more information, see symmetric cryptography[94], asymmetric cryptography[94], or Defend Dissent: What is Encryption?[97]

[94] anarsec.guide/glossary

[95] anarsec.guide/posts/linux/#the-command-line-interface

[96] techlearningcollective.com/foundations/linux-journey/the-shell

[97] open.oregonstate.education/defenddissent/chapter/what-is-encryption/

on your device are malicious. The Auditor app must be configured immediately after GrapheneOS is installed, before any Internet connection is made.

How does it work? Your new device is the *auditee*, and the *auditor* can be either another instance of the Auditor app on a friend's phone or the Remote Attestation Service[21] — we recommend doing both. The *auditor* and *auditee* pair to create a private key, and if the *auditee's* operating system is tampered with after the pairing is complete, the *auditor* will be alerted during the next test.

First, immediately after installing the device and before connecting to the Internet, perform a "local verification"[22]. This requires the presence of a friend whom you see semi-regularly and who has the Auditor app (on any Android device). The first pairing will show a brown background, and subsequent audits will show attestation results with a green background if nothing is remiss. There is no remote connection established between the phones of the auditor and auditee; you must perform these verifications in person.

We recommend using the phone as a Wi-Fi only device. Turn on airplane mode. It "will fully disable the cellular radio transmit and receive capabilities, which will prevent your phone from being reached from the cellular network and stop your carrier (and anyone impersonating them to you) from tracking the device via the cellular radio." Leave airplane mode enabled at all times — otherwise the phone will interact with cellular networks even if there is no SIM card in the phone.

You are now ready to connect to Wi-Fi. Once you have an Internet connection, we recommend that you immediately set up a scheduled remote verification[23] with an email that you check regularly. You can always log back in to view your attestation history. The default delay until alerts is 48 hours; if you know your phone will be off for a longer

[21] attestation.app/

[22] attestation.app/tutorial#local-verification

[23] attestation.app/tutorial#scheduled-remote-verification

period, you can update the configuration to a maximum of two weeks. If your phone will be off for more than two weeks (for example, if you leave it at home while traveling), simply ignore the notification emails.

If Auditor ever detects tampering, you should immediately treat the device as untrusted. Forensic analysis[24] may be able to reveal how the compromise occured, which helps to prevent it from happening again. You can get in touch with a service like Access Now's Digital Security Helpline[25], though we recommend not sending them any personal data.

User Profiles

User profiles are a feature that allows you to compartmentalize your phone, similar to how Qubes OS[26] compartmentalizes your computer. User profiles have their own instances of apps, app data, and profile data. Apps can't see the apps in other user profiles and can only communicate with apps within the same user profile. In other words, user profiles are isolated from each other — if one is compromised, the others aren't necessarily.

The Owner user profile is the default profile that is present when you turn on the phone. You can create additional user profiles. Each profile is encrypted† with its own encryption key and cannot access the data of other profiles. Even the device owner cannot view the data of other profiles without knowing their password.

We'll now create a second user profile for all applications that don't require Google Play services:

- **Settings → System → Multiple users**, press **Add user**. You can name it Default and press **Switch to Default**.

[24] notrace.how/threat-library/mitigations/computer-and-mobile-forensics.html
[25] accessnow.org/help
[26] anarsec.guide/posts/qubes/#what-is-qubes-os

from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network†. See Tails for Anarchists[87] and Tails Best Practices[88].

Operating system†: Qubes OS has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials[89]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[90].

See When to Use Tails vs. Qubes OS[91]. We do not offer "harm reduction" advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists[92]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[93].

[87] anarsec.guide/posts/tails/
[88] anarsec.guide/posts/tails-best/
[89] anarsec.guide/posts/linux
[90] anarsec.guide/posts/qubes/
[91] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[92] anarsec.guide/posts/e2ee/
[93] anarsec.guide/posts/tamper/

obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France[83]: "So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken" and must remain so, even if it's switched off, we become a potential state informer…"

You may also be interested in the Threat Library's "Digital Best Practices"[84].

Your Phone

Operating system†: GrapheneOS is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[85]. If you decide to have a phone, treat it like an "encrypted landline" and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[86].

Your Computer

Operating system†: Tails is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs

[83] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/

[84] notrace.how/threat-library/mitigations/digital-best-practices.html

[85] anarsec.guide/posts/grapheneos/

[86] anarsec.guide/posts/nophones/

- Set a password that is different from your Owner user profile password.
  - This is the profile that you will be regularly unlocking throughout the day. This means that you only have to enter the Owner password upon boot, which allows it to be very strong. For the Default password, choose either the combination of a weak password + a short locking time, or a strong password[27] + a longer locking time. The first option puts trust in the rate-limiting of password attempts enforced by the secure element[28]. The second option doesn't put trust in the rate-limiting, given it could be bypassed through a secure element vulnerability, but has the trade-off that the profile data is vulnerable if the device is left unattended while unlocked. You can also have a strong password + a short locking time if you don't unlock the device many times a day. Keep in mind that if police ever seize your device (such as during a daytime house raid), it should ideally be turned off, and at minimum, it should be locked (which starts the countdown to the Auto reboot feature mentioned below).
- In the Default user profile, you can set the locking time with **Settings → Security → Screen lock settings → Lock after screen timeout**, and the screen timeout with **Settings → Display → Screen timeout**.

Later, we will optionally create a third user profile for applications that require Google Play services.

When you press **End session** on a profile, that profile's data is encrypted at rest. A shortcut for switching between different user profiles is located at the bottom of Quick Settings (accessible by swiping down twice from the top of the screen).

To reiterate, the user profiles and their purposes are:

1) Owner

[27] anarsec.guide/posts/tails-best/#passwords

[28] grapheneos.org/faq#encryption

- Where applications are installed

2) Default

- Where applications are used

3) Google (optional)

- Where applications that require Google Play services are used

How to Install Software

The GrapheneOS app store contains the standalone applications developed by the GrapheneOS project, such as Vanadium, Auditor, Camera, and PDF Viewer. These are automatically updated.

To install additional software, Sandboxed† Google Play can be installed through the GrapheneOS app store: "Google Play receives absolutely no special access or privileges on GrapheneOS."[29]

Avoid F-Droid due to its numerous security issues[30]. The Aurora Store[31] has some of the same security issues as F-Droid[32].

The approach we will take is that all applications needed in the Default user profile will be installed in the Owner user profile, using Sandboxed Google Play. In the Owner user profile, all installed applications will be "disabled", because we only use these applications from the Default user profile (except, if you ever use the phone away from home[33], a VPN app that needs to run in all profiles). Then we'll use the **Install available apps** feature to delegate apps to the Default user profile.

[29] grapheneos.org/features#sandboxed-google-play
[30] privacyguides.org/en/android/#f-droid
[31] privacyguides.org/en/android/#aurora-store
[32] privsec.dev/posts/android/f-droid-security-issues/#conclusion-what-should-you-do
[33] anarsec.guide/posts/grapheneos/#force-all-network-traffic-through-a-vpn

Wrapping Up

With the set-up described in this guide, if a cop starts with your name, they won't be able to simply look it up in a cellular provider database to get your phone number. If you use the phone as a Wi-Fi only device and always leave it at home, it cannot be used to determine your movement profile and history. If you use a VoIP number accessed through a VPN, even if that number is known it can't be used to locate you. All communications with comrades use end-to-end encryption[74] so they do not facilitate network mapping[75]. Even if you are unlucky enough to be targeted by a well-funded investigation, the hardened operating system makes it difficult to compromise with spyware, and such a compromise should be detectable[76].

By storing the phone in a tamper-evident manner when it's not in use, you'll be able to tell if it's been physically accessed. See the guide Make Your Electronics Tamper-Evident[77].

The GrapheneOS forum[78] is generally very helpful for any remaining questions you may have.

For information on burner phones, see the No Trace Project[79].

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[80] for the purposes of incrimination[81] and network mapping[82]. Our goal is to

[74] anarsec.guide/posts/e2ee/
[75] notrace.how/threat-library/techniques/network-mapping.html
[76] anarsec.guide/posts/grapheneos/#auditor
[77] anarsec.guide/posts/tamper/
[78] discuss.grapheneos.org/
[79] notrace.how/threat-library/mitigations/anonymous-phones.html
[80] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[81] notrace.how/threat-library/tactics/incrimination.html
[82] notrace.how/threat-library/techniques/network-mapping.html

up files by copying them to a USB-C flash drive using the Files app, or sending them to yourself using an encrypted messaging app[67].

Password Management

If you feel you need a password manager, KeePassDX[68] is a good option. However, most app credentials can be stored in KeePassXC[69] on a computer because they don't need to be entered regularly. The setup described in this guide requires memorizing two passwords:

1) The Owner user profile (boot password)
2) The Default user profile
3) (Optional) Apps like Cwtch[70] and Molly[71] have their own passwords.

For advice on password quality, see Tails Best Practices[27].

Linux Desktop Phones

Why recommend a Pixel over a Linux desktop phone? Linux desktop phones like the PinePhone Pro[72] are much easier to hack than GrapheneOS[73] because they lack modern security features like full system MAC policies, verified boot, strong app sandboxing, and modern exploit† mitigations. Their hardware architecturally lacks modern security features like hardware based encryption (via a Trusted Execution Environment/Secure Element) and has questionable integration of components such as the modem.

[67] anarsec.guide/posts/e2ee/
[68] privacyguides.org/en/passwords/#keepassdx-android
[69] anarsec.guide/posts/tails/#password-manager-keepassxc
[70] anarsec.guide/posts/e2ee/#cwtch
[71] anarsec.guide/posts/e2ee/#signal
[27] anarsec.guide/posts/tails-best/#passwords
[72] en.wikipedia.org/wiki/PinePhone_Pro
[73] madaidans-insecurities.github.io/linux-phones.html

Software from Sandboxed Google Play

To install and configure Sandboxed Google Play:

- In the Owner user profile, install Sandboxed Google Play by opening Apps and installing Google Play services (this will also install the Google Services Framework and the Google Play Store).
- The Google Play Store requires a Google account to sign in, but one with false info can be created for exclusive use with the Google Play Store.
- Once installed and signed in, disable the advertising ID: **Settings → Apps → Sandboxed Google Play → Google Settings → Ads**, and select *Delete advertising ID*.
- Automatic updates are enabled by default on the Google Play Store: **Google Play Store Settings → Network Preferences → Auto-update apps**.
- Notifications for Google Play Store and Google Play Services must be enabled for auto-updates to work: **Settings → Apps → Google Play Store / Google Play Services → Notifications**. If you get notifications from the Play Store that it wants to update itself, accept them[34].

You are now ready to install applications from the Google Play Store. See Encrypted Messaging for Anarchists[35] for ideas.

Delegating apps

Now we will delegate apps to the profiles they are needed in:

- In the Owner profile, disable all applications downloaded from the Play Store (except for the VPN): **Settings → Apps → [Example] → Disable**.

[34] discuss.grapheneos.org/d/4191-what-were-your-less-than-ideal-experiences-with-grapheneos/18
[35] anarsec.guide/posts/e2ee/

- To install any app in the Default user profile: **Settings → System → Multiple users → Default → Install available apps**, then select it.

Software That Isn't On the Play Store

Some apps are not on the Play Store, either because they're still in development or because they don't want users to have to interact with Google. Apps installed through the Play Store update automatically, but if you were to download individual APK installer files, you would have to remember to update them yourself (there are exceptions, like Signal, which is designed to update itself). Additionally, you must verify the authenticity of the APK file yourself with a tool like AppVerifier[36].

Obtainium[37] is an app manager which allows you to automatically update apps after installing them from an APK file (an APK is found from the developer's own releases page such as GitHub or the developer's website). It is available on their GitHub Releases page[38] — `app-arm64-v8a-release.apk` of the latest release is what you want (arm64-v8a is the processor architecture). If you need apps that aren't available in the Play Store, install Obtainium in the Owner user profile (and don't disable it). Use the same process as above to install apps into the Owner user profile, but through Obtainium, then disable the app and delegate it to a secondary profile. AppVerifier integrates with Obtainium so that before Obtanium installs an APK you can do a verification — AppVerifier can approve selected apps, or you can manually compare the APK's fingerprint to somewhere that the developer has published it.

As an example of how to use Obtainium, Molly-FOSS is a hardened version of Signal without Google software[39] and it is available from

[36] github.com/soupslurpr/AppVerifier
[37] privacyguides.org/en/android/#obtainium
[38] github.com/ImranR98/Obtainium/releases
[39] github.com/mollyim/mollyim-android#free-and-open-source

In all profiles:

- Leave the Global Toggles for Bluetooth, location, camera access, and microphone access disabled when you don't need them for a specific purpose. Apps cannot use disabled features (even with individual permissions) until they are re-enabled. Also set a Bluetooth timeout: **Settings → Connected devices → Bluetooth timeout:** 2 minutes
- In the "Messaging" app, disable **Settings → Advanced → Auto-retrieve**
- Many applications allow you to "share" a file with them for media upload. For example, if you want to send a picture on Signal, do not grant Signal access to "photos and videos" because it will have access to all of your pictures. Instead, in the Files app, long-press to select the picture, and then share it with Signal.
- When an app asks for storage permissions, select Storage Scopes[63]. This will make the app think that it has all the storage permissions it is requesting, when in fact it has none. The same is true for Contact Scopes[64].

How to Backup

Don't use cloud backups. You can't trust the corporate options, and they're the easiest way for the police to access your data. If you must back up your phone, back it up to your encrypted computer.

GrapheneOS currently offers Seedvault[65] as a backup solution, but it's not very reliable. As the documentation notes[66], connecting directly to a computer requires "needing to trust the computer with coarse-grained access", so it is best to avoid it. Instead, you can manually back

[61] grapheneos.social/@GrapheneOS/112204443938445819
[62] grapheneos.social/@GrapheneOS/112204446073852302
[63] grapheneos.org/usage#storage-scopes
[64] grapheneos.org/usage#contact-scopes
[65] grapheneos.org/features#encrypted-backups
[66] grapheneos.org/faq#file-transfer

through the Tor network, but simply using the Vanadium browser through Orbot is not recommended by the Tor Project[59].

Recommended Settings and Habits

Turn off the phone overnight and when you leave it at home. Full Disk Encryption† is most effective when the device is turned off. Additionally, if the operating system is compromised by malware† a reboot can clean the malware from your system[60], so it is best practice to shut down the device daily.

In the Owner user profile:

- **Settings → Security → Auto reboot:** 18 hours or less
  - The automatic reboot, if no profile has been unlocked for several hours, will put the device fully at rest again. It will reboot overnight if you forget to turn it off. If the police ever manage to get their hands on your phone while it is in a lock-screen state, this setting will return it to more effective encryption once the time has elapsed[61].
- **Settings → Security → USB-C Port:** Charging-only or Off[62]
- **Settings → System → Multiple users → [Username] → App installs and updates:** Disabled
  - Once you have all the applications you need in a secondary user profile, disable app installation in that profile — apps that are delegated to a secondary user profile from the Owner profile (via "Install available apps", as described above) will still be updated.
- **Settings → System → Multiple users:** Send notifications to current user (enabled)
  - It is convenient to be able to receive notifications from any user profile:

[59] support.torproject.org/tbb/tbb-9/
[60] privacyguides.org/en/os/android-overview/#verified-boot

Github Releases[40]. In Obtanium, press **Add App**, then paste the Github Releases URL.

Software That Requires Google Play Services

If there is an app you want to use that requires Google Play services, create another secondary user profile for it. This is also a good way to isolate any app you need to use that isn't open-source† or reputable. You will need to install and configure Sandboxed Google Play in this "Google" user profile.

Many banking apps[41] will require Sandboxed Google Play. However, banking can simply be accessed through a computer to avoid the need for this "Google" user profile.

VoIP

A Wi-Fi only smartphone doesn't require a service plan. As explained in Kill the Cop in Your Pocket[42], bureaucracies often require a phone number that can be called from a normal phone (without encryption). VoIP† applications allow you to create a number and make calls over Wi-Fi rather than through cell towers. A phone number is also occasionally required to register for an application, and a VoIP number will usually work.

Some of the VoIP applications that work on computers[43] also work on smartphones. The jmp.chat[44] VoIP service can be paid for in Bitcoin, and it can be used with their Cheogram app[45]. There are also mobile-only paid options such as MySudo (although it only works in a handful

[40] github.com/mollyim/mollyim-android/releases
[41] grapheneos.org/usage#banking-apps
[42] anarsec.guide/posts/nophones#bureaucracy
[43] anarsec.guide/posts/nophones#bureaucracy
[44] kicksecure.com/wiki/Mobile_Phone_Security#Phone_Number_Registration_Unlinked_to_SIM_Card
[45] cheogram.com/

of countries[46]). A MySudo subscription can be purchased anonymously with Google Play gift cards[47], but this is probably unnecessary if the point is to give the number to bureaucracies. MySudo requires Google Play Services.

Force All Network Traffic Through a VPN

It is best to force all of GrapheneOS's network traffic through a VPN[†] — this puts your trust in your VPN instead of an inherently untrustworthy Internet Service Provider. As the Security Lab[48] notes:

> Using a reputable VPN provider can provide more privacy against surveillance from your ISP or government and prevent network injection attacks from those entities. A VPN will also make traffic correlation attacks — especially those targeting messaging apps — more difficult to perform and less effective.

There are two ways you can run a VPN: from your phone or from your networking device (either a router or a hardware firewall). When using your phone from home, we recommend the latter.

It's unnecessary to "double up" a VPN — if its running on your networking device, it doesn't need to be running on your phone, and vice-versa. This means that a phone running a VPN should disable it before connecting to Wi-Fi configured with a "VPN Kill Switch".

If you ever use the phone away from home, you should configure GrapheneOS to force all network traffic through a VPN — install the

[46] support.mysudo.com/hc/en-us/articles/360019983274-Which-countries-are-supported-for-Sudo-phone-numbers

[47] support.google.com/googleplay/answer/3422734

[48] securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

VPN app in every user profile. All standard GrapheneOS connections will be forced through the VPN (except for connectivity checks[49], which can be optionally disabled[50]). Note that **Always-on VPN** and **Block connections without VPN** are enabled by default on GrapheneOS. Keep in mind that you'll want to disable the VPN app before connecting to your home's "VPN Kill Switch" Wi-Fi.

If you can afford to pay for a VPN, we recommend both Mullvad[51] and IVPN[52]. Otherwise, you can use RiseupVPN, although it has far fewer users to blend in with, and it doesn't meet several important security criteria for VPN providers[53], such as published security audits of its code and infrastructure. A VPN subscription should be purchased anonymously — vouchers are available from Mullvad[54] and IVPN[55] to purchase the subscription anonymously without Monero[56].

Tor

You may want to use Tor[†] from a smartphone. However, if you need the anonymity of Tor rather than the privacy of Riseup VPN, you should use either Qubes OS or Tails[57] on a computer. The Graphene docs[58] recommend avoiding Gecko-based browsers like Tor Browser, as these browsers "do not have internal sandboxing on Android." Orbot is an app that can route traffic from any other app on your device

[49] grapheneos.org/faq#default-connections

[50] privsec.dev/posts/android/android-tips/#connectivity-check

[51] privacyguides.org/en/vpn/#mullvad

[52] privacyguides.org/en/vpn/#ivpn

[53] privacyguides.org/en/vpn/#criteria

[54] mullvad.net/en/blog/2022/9/16/mullvads-physical-voucher-cards-are-now-available-in-11-countries-on-amazon/

[55] ivpn.net/knowledgebase/billing/voucher-cards-faq/

[56] privacyguides.org/en/cryptocurrency/#monero

[57] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

[58] grapheneos.org/usage#web-browsing