GrapheneOS Phone Startup Guide

Updated May 2024
GrapheneGoat.com

a special thanks to freedomtech.com.au for making some of the detailed instructions in this guide

** If you cannot get into your new phone after purchase/arrival, message me at: phones@graphenegoat.com to get the PIN your phone shipped with. We do this to ensure that your new device was not tampered with during transport. **

Thank you for purchasing a new GrapheneOS phone, this guide will walk you through setup and provide a basic start into using this new secure device. On your specific builds, we have installed several app stores to get you started quicker, F-Droid and Aurora Store. Please check all of your settings on the device and adjust to your needs, the phone is Android still, so for Android users, you will notice that the settings menu looks nearly identical, and is fairly straightforward. Those coming from iPhone will have a little bit of a learning curve, but once you get familiar with this device, you will be comfortable on just about any other Android device, whether it's GrapheneOS or not.

GrapheneOS is an Android-based, security-hardened, privacy-focused, free, open-source mobile operating system for selected smartphones, the device you have is a 128/256GB Google Pixel __ which is 4G LTE / 5G, and are generally waterproof against most spills or drops in shallow water. GrapheneOS is focused on privacy and security by default. This guide will help walk you through basic settings and setup, step by step, and for any problems, advice or questions, please reach out to us at phones@graphenegoat.com or at graphenegoat@protonmail.com if you want encrypted email chat.

~

Setting up GrapheneOS upon startup:

Power on your de-Googled phone by pressing the small colored button on the right of the frame for several seconds. This will bring up a warning: '**Your device is loading a different operating system.'**

- The power button will have a message to press to pause. You can either wait a moment or press the power button and then press it again, which will start the boot process.

- The Google logo will then show, which is normal. This is part of the bootloader process. You are not installing any Google software on the phone. They are just the manufacturer that we are going to happily ignore.

- Next, it will show the GrapheneOS start screen.
- Your phones have already been through basic setup, so some of the following first steps have already been completed, however you can change anything at anytime via the Settings menu.

Please Note: before pressing Start for this process, you will notice an option called **Accessibility Settings** on the bottom right of the screen. This option would typically take you to a screen to change the settings for those that are vision impaired—things like font size, display size, and magnification customizations. We suggest skipping that for now, as you may change the accessibility options later in the settings menu.

- Now commence the initial setup through the following screens:

- **Language:** Set to your Country and Language - default is English (United States)

- **Time and Date:** Set the time zone, date, and time to your location. <mark>(Your phone has been set to Pacific Time on initial setup, please adjust as needed.)</mark>

- **Wi-Fi:** Connect to an accessible Wi-Fi network – the available networks will automatically be visible - connect to the best for your circumstances.

Special Notes:

Network Preferences
When you turn on your de-Googled phone, the Wi-Fi automatically toggles on. If ON, it will connect automatically to known Wi-Fi such as home/work. If OFF, you will need to connect manually. We usually set our toggle to OFF to ensure we are not joining a network unless by choice.

While a good VPN should give you protection, if you toggle to ON, this will also turn on Wi-Fi scanning, so your phone will constantly be scanning for Wi-Fi which we appreciate many people do not want.

Insert SIM Card
This step can be skipped while you set up the phone if you set up and download your apps via Wi-Fi.

Cell Data
Assuming you don't have access to Wi-Fi, if you want to use cellular data in the setup process, you will need to insert a SIM. If you are inserting a new SIM, you may need to register with the Provider. Charges may apply depending on the data used.

Location Services
Decide if you want apps to be given automatic location access in your GrapheneOS setup. We typically deny and modify specific permissions on an app-by-app basis. <mark>I turned off the global Location setting on initial setup, so you will need to toggle on Location for any app that requires it. This way the phone's location is OFF unless you specifically turn it on, or grant an app permission to use it.</mark>

Secure Your Phone
Decide what kind of security you want to employ to allow your device to unlock. A fingerprint or face recognition (if your phone model supports these), a PIN and/or a password. You should set up at least one of these security features to prevent unauthorized access to your phone.
<mark>*Your phone's PIN will be sent to you at time of purchase to ensure your phone is secure during transport. If you don't have the PIN, email us at: phones@graphenegoat.com</mark>
To change your PIN, go to Settings > Security > Screen lock and enter your new PIN or passcode

There are several in-built security features in GrapheneOS. The first is setting the pin to scrambling. Scrambling allows the numerals of the keypad to show at random positions each login. Scrambling helps from people overlooking you keying in a code and guessing the digits.

To enable this, navigate to **Settings** > **Security** > **PIN Scrambling** and toggle this to **On**.

Restore Apps and Data
The final setup screen allows you to restore any apps and data from a previous GrapheneOS phone. Connections for this include a USB flash drive and Nextcloud. We expect those using this guide would not have an earlier GrapheneOS phone, so you may skip this step.

~

Step 2: Initial Start of GrapheneOS

As keen as you will be to get things moving and downloaded, now is the best time to make initial tweaks to the phone to make it more user friendly before launching on the Internet.

First is the navigation of menus. In this short time, you may have noticed that the swipe control is different from what you used in the past. Here are a few guidance points to help you navigate your new de-Googled phone.

System Navigation
By default, GrapheneOS uses gesture-based navigation. Your phone has been setup for '3 Button Navigation' but can be changed to Gesture. *2 Button Navigation is now no longer available.*

The system navigation mode can be configured in **Settings** > **System** > **Gestures** > **System navigation**.

The same Menu is also available in **Settings** > **Accessibility** > **System controls** > **System navigation**.

Gesture Navigation
The bottom of the screen is a reserved touch zone for system navigation. A line is displayed in the centre to show that the navigation bar is present across the entire bottom of the screen. In most apps, this area will display padding.

The Home gesture is swiping up from the navigation bar while removing your finger from the screen.

The Recent Apps gesture is swiping up from the navigation bar while holding your finger on the screen before releasing.

The most recently opened activity is always on the furthest right. Each step left goes one step back through the history of recently opened apps. Opening an app with the recent App's activity will place it on the furthest right in the recent App order, just like opening a new App.

The recent app activity has a screenshot button as an alternative to holding power and volume down while using an app.

Rather than opening the recent App's activity, you can swipe left on the navigation bar for the Previous App and swipe right for the Next App. This will not change the recent App's order. This is usually the best way to navigate through recent apps.

Swiping from either the left or the right of the screen within the App (not the navigation bar) is the Back gesture.

Apps are supposed to avoid implementing conflicting gestures but have the option to override this gesture if they genuinely need to get rid of it. You can avoid triggering the back gesture in one of 2 easy ways:

- Avoid swiping from right near the edge
- Hold your finger on the side of the screen for a moment before swiping.

The more advanced option is using a diagonal swipe pointing sharply to the bottom of the screen since this will bypass the back gesture but will still trigger most app gestures. The advanced option is the most convenient approach once you get used to doing it.

The launcher uses a swipe-up gesture starting anywhere on the screen to open the app drawer from the home screen. You need to start that gesture above the system navigation bar since any gesture starting on the navigation bar is handled by the OS as a system navigation gesture.

3-Button Navigation
3-button navigation is Android's oldest touchscreen-based navigation system. It will remain supported for the foreseeable future to provide accessibility for users unable to easily use the gestures. It's older than 2-button navigation but isn't considered a legacy feature.

A large row across the bottom of the screen is reserved for navigation buttons. The Back button is on the left, the Home button is in the center, and the Recent Apps button is on the right.

The most recently opened activity is always on the furthest right in the recent App's activity. Each step left goes one step back through the history of recently opened apps. Opening an app with the recent App's activity will place it on the furthest right in the recent App's order, just like opening a new app.

The recent app activity has a screenshot button as an alternative to holding power and volume down while using an app.

System Tweaks
We use these settings on our company phones and find them most popular with our clients. They are changes to the default settings that you may wish to explore. We find they help with the ease of viewing and everyday use.

We will go into the **Settings** menu and make our way through the basics. Once we have set the framework, we will look at the Apps we are going to install, and then, depending on the choices made, we will come back and tighten it up.

Network and Internet
- **Settings** > **Network & Internet** > **Data Saver Toggle** to **ON** if you have limited data.
- Only use this if necessary, as it can slow some apps down.

Battery
- **Settings** > **Battery** > **Battery Percentage** toggle to **ON**. (COMPLETED)
- This will show the percentage of battery life left in the notification bar.

Sound
- **Settings** > **Ring and notification volume** > slide to **1/2** volume.

Display
- **Settings** > **Display** > **Adaptive brightness** toggle to **ON**

- **Settings** > **Display** > **Lock screen** > **Privacy** > **Don't show notifications at all.**
- Who wants strangers or colleagues to see your notifications?

- **Settings** > **Display** > **Lock screen** > **Tap to check phone** > toggle to **OFF**.
- It is just as easy to press the power button.

- **Settings** > **Display** > **Lock screen** > **Double Line Clock**> toggle to **ON**.

- **Settings** > **Display** > **Lock screen** > **Lift to check phone** > Toggle to **OFF**
- As above, it is just as easy to press the power button

- **Settings** > **Display** > **Lock screen** > **Wake screen for notifications** toggle to **OFF**
- You don't want to be continuously distracted when the phone is next to you, constantly asking for attention.
- **Settings** > **Display** > **Screen timeout** default to 2 minutes**.**

- **Settings** > **Display** > **Night Light** > **Use Night Light** toggle to **ON**.

- **Settings** > **Display** > **Night Light** > **Will not turn off automatically** > tap **Do not use sunrise and sunset times** as this means you need to give location access.
- Instead, use **Schedule** and set your custom start and end time.

- **Settings** > **Display** > **Auto-rotate screen** toggle to **ON.**

- **Settings** > **Display** > **Increase touch sensitivity**. (Not available on Pixel 3)
- You may want to toggle to **ON** if a thick screen protector is used.

- **Settings** > **System** > **Languages & input** > **On-screen keyboard** > **GrapheneOS keyboard** > This will show Languages/ Engish (US).
- This is only for the layout of the keyboard, so it is all perfectly good.

- **Settings** > **System** > **Languages & input** > **On-screen keyboard** > **GrapheneOS keyboard** > **Preferences** > **Vibrate on keypress** toggle to **OFF**.

- **Settings** > **System** > **Languages & input** > **On-screen keyboard** > **GrapheneOS keyboard** > **Appearance & Layouts** > **Theme** then **Material Dark**.
- This allows the keyboard to be seen more quickly.

- **Settings** > **System** > **Languages & input** > **On-screen keyboard** > **GrapheneOS keyboard** > **Text correction** > **Personalised suggestions** toggle to **ON**.
- This is kept only in the phone and not shared with outside parties.

- **Settings** > **Security** > **Screen lock** > set your preferred login PIN / Password.

- **Settings** > **Security** > **Face Unlock / Fingerprint** > We usually leave this off.

- **Settings** > **Security** > **PIN scrambling** > toggle to **ON**.
- This allows the numerals of the keypad to show at random positions for each login. This helps from people overlooking your keying in a code and guessing the digits.

- **Settings** > **Security** > **Screen lock camera access** > toggle to **OFF**.
- This means you cannot accidentally take videos but also helps lockdown any unwanted intrusion. ***If you believe you may be in a situation where you may need to document an event instantly, you may wish to change this setting prior, then revert.**

Step 3 - App Installations

Finally, we are getting something on our phone, the apps that make our lives easier and enslave us to Big Tech if not installed correctly. The fact is, we are like children without parents when it comes to technology. We know vegetables are good for us, but damn, those lollies and sweets are so good we just can't fit any other food in!

There are three ways to go here. Reckless, Careful, and Cautious. The way we see it, we have already gone this far, so we might as well be cautious.

Reckless Option for Apps
This involves quickly getting apps from the Google Play store and deleting the account.

Careful Option for Apps
Here you would set up another account on this phone is a "sandboxed" environment. It is like having a quarantine ward in your phone that can reach the outside world but has no access to the rest of the hospital. This ward only contains malicious apps that may affect your privacy.

Cautious Option for Apps
This is the best way to ensure your privacy. We will be installing apps from 3 sources - F-droid, Websites, and Aurora Store.

- F-droid is a repository of free and open-source (FOSS) apps. Apps here have minimal permissions, and as they contain no trackers, you can be assured of a high level of privacy. This is our premium source of preferred Apps. This site can be reached at <u>www.f-droid.org</u>. (INSTALLED)

- For downloading from websites, we don't necessarily suggest going to a website and downloading their App. Most of the time, you will be diverted back through to Google, which defeats the purpose of going down the privacy route. By websites, we mean something similar to Gab, or perhaps a weather page. This is where you get a shortcut on your screen or bookmark a site instead of installing an app.

- Aurora Store is a popular open-source client of the Google Play Store, allowing users to search, download, and update Android apps and games on any device. You will need to download the Aurora Store app and then explore. (INSTALLED)

~

Step 4 - Internet & Browser

Okay, we admit some of this is technical and can be tedious, but before we jump on the Internet and start downloading, some decisions are to be made regarding our DNS servers, Virtual Private Networks (VPN's), Web browsers, and our Search engines.

Even though they are all different components, they all tie into each other, and the choices here may have a significant impact on our privacy. Unless we get it right, we may not be utilizing the full benefit of going to a de-Googled phone.

At the time of this writing, Proton VPN with NextDNS works excellent on GrapheneOS (make sure to turn off Netshield within the Settings in Proton VPN if you choose a custom DNS), not all DNS / VPN combinations will play well with each other. Vanadium is the default browser, but we think Brave and Tor also have good use cases and recommend keeping those on the device in addition to Vanadium.

Ad-blocking

No one likes ads. They remind us of bothersome flies. The ones that land right where you are reading. When you try to brush them away, they are back again, but with a vengeance.

The difficulty with ad-blockers is that you are limited to 3 methods of using them: A private DNS (Domain Name Server) service, a Paid or free ad-blocker extension, or an ad-blocking browser. However, as many of our apps will be coming from F-droid, we will not be experiencing as many problems as we would through the regular Google Play Store. That means far less add tracking.

Private DNS Service

A DNS (Domain Name Server) is the Postman of the Internet. We can type in a website (domain) name (such as www.cloudflare.com,) and we are delivered to the IP address of that site (1.1.1.1).

This is similar to a translator, taking our human words and translating them into computer-read Internet Protocol (IP) addresses.

The problem is that your network provider typically provides the Postman and the DNS. They usually take a note (log) of every site you visit. They may sell your browsing history to third parties.

We have an option to override this in our settings and nominate a DNS server of our choice.

The good thing about this is that some DNS providers are interested in our privacy, maintain that they do not keep records, and actually block ads, such as DNS ad-guard.

The issue with this solution, as noted at https://grapheneos.org/faq#default-dns, is that, in fact, using the network-provided DNS servers from your mobile carrier is the best way to blend in with other users, therefore not standing out.

This means Networks and websites can fingerprint and track users based on a non-default DNS configuration.

The GrapheneOS recommendation for general purpose usage is to use the network-provided DNS servers.

The fall-back DNS server, in case the first one is not working, defaults to Cloudflare. Most Android phones fall back server defaults to Google, so by not going through Google, you will also retain privacy if there is a problem with your primary DNS.

In summary, if we have a Private DNS, we risk being identified by standing out, but the benefit is having our ads blocked and being able to filter out nearly anything we wish at a very granular level. NextDNS is a great option if you choose to use a custom DNS provider.

If you decide to Install a Private DNS service, navigate to **Settings** > **Network and Internet** > **Private DNS** > **Private DNS provider hostname** > then type in your server's name. Note, it is your Servers name, not IP address (so dns.ad-guard.com).

****
<mark>Your phone can be setup to use your own instance of NextDNS, see our page on how to do this anonymously here:</mark>

<mark>https://graphenegoat.com/grapheneos-phones/nextdns/</mark>

<mark>If you do not wish to use NextDNS, visit Settings>Network & Internet>Private DNS and select 'Automatic' to return to default later if you change your mind.
NextDNS allows you to filter out ads, malware and anything else you prefer upstream of the phone itself, saving you battery, and offering some anonymity.</mark>
****

Ad-blocking Extension
GrapheneOS comes with a hardened Browser, **Vanadium**, which has been built entirely with security in mind.

GrapheneOS's official position is against trying to achieve browser privacy and security through piling on browser extensions and modifications. They note that adding extensions or changes to the default settings only helps isolate you as a user and generally provides more ways to track you.

Ad-blocking Browser
As noted on their usage page https://grapheneos.org/usage#web-browsing, Chromium-based **Bromite** is a solid alternative to their default browser Vanadium and is the only other browser they recommend.

Bromite provides integrated ad-blocking and more advanced anti-fingerprinting. For now, Vanadium is more focused on security hardening, and Bromite is more focused on anti-fingerprinting. The projects are collaborating together and will likely converge to provide a combination of the best features.

As things stand, it seems we have 2 main choices. We will discard the idea of putting an ad-blocking extension onto the default browser, Vanadium. We will only be getting a few ads from websites etc. Therefore it is not worth compromising our anonymity.

So, DNS, or Ad-blocking browser? Before deciding, let's throw another computation into the mix. VPN.

VPN Service
Every mobile carrier is going to log the use of your data and any website you visit. The Provider of any Wi-Fi you access will also log the use of your data and the website you visit. These records must legally be kept for years, depending upon the jurisdiction, and the metadata turned over to authorities if requested.

A VPN connects your phone, tablet, or PC to a server on the Internet and allows us to browse the Internet using that computer's internet connection and IP address. This encrypts the network traffic between your device and the VPN provider and will help cloak information from your internet provider.

All that your Provider's logs will record is an encrypted communication between your device and the VPN server and not the sites you have visited. As for the outside world, the places we see on the web, if our VPN server was in Singapore and we were in the United States, then we would appear to be in

Singapore. Our own IP address (our computer number) would be hidden. The world would only see the Singapore server address.

If we visit back to the postman analogy. With a VPN, we have an encrypted connection between us and our "pretend" location in Singapore. Our Singapore connection will ask the Postman to deliver us to an address. The Postman sees us in Singapore because that is who is making the request.

One of the problems with a VPN, is that data speed can slow if your VPN is too far away. The benefit is to provide another layer of anonymity, and that can only be good.

Keep in mind that not all providers are equal. They can still see your movements and monitor your traffic, and some well-known VPNs have been recently acquired by Big Tech or other phantom companies. As a result, questions have been raised about their new owners.

Still, a VPN will encrypt your network traffic between your device and the VPN provider. It will help cloak information from your internet provider, who is probably more likely to sell or hand over your browsing history data than a well-researched VPN provider.

Oh, and did we mention that they also tend to be ad-blocking? So yes, a VPN service for me!

VPNs We Currently Recommend -in no particular order, Proton or Mullvad are preferred. Proton has a free tier offering if you don't wish to pay for a VPN, however you won't have as fast of a speed. A paid VPN is a must these days, it is highly recommended to purchase and use one of these:

- ProtonVPN https://protonvpn.com/is best known for their private proton mail service.

- Mullvad VPN https://mullvad.net/en/ ($5/month fixed rate)

Each of these VPNs recommended has a strict no-logging policy, meaning they commit not to record traffic, however we must remember that while a VPN is extremely valuable for privacy and security, it is not bulletproof at remaining truly anonymous.

Internet & Browser Summary
The above information leads to our recommendation to use an ad-blocking browser with a VPN, and between them both, we should have the privacy of location, be ad-free, and reasonably cloaked in anonymity. Adding custom DNS makes us more unique, but offers more control of what can be easily filtered out, not just ads but specific connections and websites.

The Brave browser also incorporates private search engines. The Brave search engine is an excellent browser option as well, Brave and Vanadium are my go to choices most of the time, however I try to use the Tor browser as much as possible also, unfortunately it is slow and not as convenient.

Privacy Browser (available from F-Droid) uses Mojeek search engine, which returns incredibly more unbiased search results, compared to using Google as your search engine.

We have also been using Startpage search engine, which has proved reliable, safe, and private as it is using Google search through a proxy. Remember that Startpage sends anonymized requests to Google, and though Google may not know who you are, they will still only send the links to pages they want you to see.

Startpage doesn't keep any data such as search requests, record IP addresses, or serve any tracking or identifying cookies. And as they are based in the Netherlands, any requests for information, not that they have any information, have to come from the Dutch Judicial authorities.

*However. Please also consider that as Startpage uses Google (anonymously) as the search engine, this may return the results as offered by Google!

<mark>***Tor has also been installed</mark>, this is The Onion Router, or 'dark web' which can access not only regular internet, but Onion address sites as well. (sometimes called Tor hidden services, usually with a '.onion' address. If you use this while not protected by a VPN, this behavior is noted by your ISP (cell carrier) so use carefully if this is a concern to you. This is an anonymous way to use the internet, however there are still methods that can identify you.

It is recommended to never use Tor to sign into anything tied to your true identity, such as email. However, Tor is a great tool to conduct anonymous searches, especially when behind a VPN. Using Tor while connected to your VPN can be very slow, but hides your searches from the ISP, and also hides the fact that you are using Tor from the ISP as well.

Conclusion
We are keeping the default DNS settings, using Brave or Vanadium as the default browser, and recommending installing a VPN service such as Proton or Mullvad. If you decide just to keep the default Vanadium browser, we will be setting that up next so we can safely access the Internet to download the initial services and apps we need, F-droid, your VPN of choice, Aurora store, and Brave browser.

~

Setting Up Vandadium

We need to give Vanadium permission to install unknown apps. In this instance, they are all unknown to our phone and browser.

Navigate to **Home page** > **APP Quick Access** bar at the bottom of the page > Press the **Browser Icon** for a few seconds (this is the tri-colour circle icon to the right of the setting icon)> Click the **information** icon > **Scroll down** and enable Allow from this source Toggle to **ON.**

~

Installing F-Droid <mark>(INSTALLED)</mark>

As previously discussed, Apps from F-Droid are free and open-source, minimize permissions, and do not have built-in-app trackers, thus assuring a high level of privacy.

- In the Vanadium browser, navigate to www.f-droid.org

- Close to the top of the page will be a Download f-droid tab

- Choose where to download Menu will open. It will show the file F-Droid.apk, and where to download it.

- Accept the default, which should be the Downloads folder.

- Click the Download button.

- At the bottom of the screen, a popup will advise that this type of file can harm your device. Do you want to keep F-Droid.apk anyway? Yes, click okay.

- The file will download, and a green tick will show. (If you are distracted and miss it - on the home page quickly scroll up which will take you to all the installed apps. Click on "files", then f-droid.apk and install)

- Click Open

- A Message will pop up. Do you want to install this App? Yes, Click Install

- Once the app is installed, click okay, and close the browser.

- The first time you go to use f-droid to install you will be asked if you want to allow from this source. Click allow.

Please note: Sometimes, if you do not press download anyway, it will default to another (donate page) page, so you will need to go back and request the download again. At other times, unless you click the instructions in quick succession it will also not download.

To update f-droid on the Home screen, open F-Droid and a message may pop up that it was designed for an earlier version of Android. It will then update the repositories. Once updated, it is ready to use.

You may wish to open F-Droid and click on the settings button. Here you can make personalized changes. The toggle switch that will show available updates is the main thing to note. As we are in a locked-down environment, the phone will not automatically update apps, so a notification in the bottom bar of this App will show if this is kept on.

Now maybe a good time to scroll around the App to look at the available download content. This will include free VPN services Proton & Calyx; if you have decided on installing a free VPN service.

~

Installing the Proton VPN Service

- On the home page, find and click to open the F-droid App, which will take you directly to the repository you were looking at earlier.

- At the bottom right of the screen is a search icon, tap it to open the search bar.

- Type in Proton.

- Click on the App.

- A message will come up. Do you want to install this App? Click Install.

- A message will come up. For your security, your phone is not allowed to install unknown apps. To allow from this source change in Settings.

- Click Settings (in the open message).

- Toggle Allow from this source to ON.

- Click the back arrow at the left top of the screen.

- Click Install.

- Open the Proton VPN.

- Sign into your account (unless using only the free version)

- Go back to Home screen Settings > Network and Internet > VPN > tap Proton > Always-on VPN toggle to ON and Block connections without VPN toggle to ON.

- Go back to Home screen Settings > Apps > All apps > Proton VPN > tap Notifications and toggle to OFF.

~

Installing the Mullvad VPN Service

- On the home page, find and click to open the F-droid App, which will take you directly to the repository you were looking at earlier.

- At the bottom right of the screen is a search icon, tap it to open the search bar.

- Type in Mullvad.

- Click on the App.

- A message will come up. Do you want to install this App? Click Install.

- A message will come up. For your security, your phone is not allowed to install unknown apps. To allow from this source change in Settings.

- Click Settings (in the open message).

- Toggle Allow from this source to ON.

- Click the back arrow at the left top of the screen.

- Click Install.

- Open the Mullvad VPN.

- Tap Create account at the bottom of the screen. You may need to retry this if you have only just installed the App.

- Note your account number, then tap Buy Credit, and purchase for the amount of time and payment of your choosing. Note that you avoid giving personal details if you pay by Bitcoin, unlike paying with a credit card.

- Select the country you wish to pop out in. We try to use somewhere relatively close. The further the distance, the less the bandwidth and speed you will get while browsing.

- Tap OK for a connection.

- Wait for the Secure Connection notification. It will also advise the City you are in.

- Click on the Settings icon at the top right.

- Click Preferences.

- Auto-connect toggle to ON, and make a choice regarding local network sharing.

- Go back to Home screen Settings > Network and Internet > VPN > tap Mullvad > Always-on VPN toggle to ON and Block connections without VPN toggle to ON.

- Go back to Home screen Settings > Apps > All apps > Mullvad VPN > tap Notifications and toggle to OFF.

This just prevents the status from being shown in Notifications which becomes annoying. It will always remain on, and if it does turn off, you will be notified. The Icon will still show active.

~

Installing the Aurora Store <mark>(INSTALLED)</mark>

The Aurora Store is a FOSS client for the Google Play Store, serving an almost identical function, allowing you to directly download apps anonymously. You can use it to install apps that are available for free in the Google Play Store.

Typically many of the trackers and permissions associated with Google have been removed. When "logging in" it spoofs your address. That means you can log in anonymously, and it will automatically make an address such as Jane.doe@gmail, the next time as john.doe@gmail, etc., without it ever knowing your true identity.

- In F-Droid, find and install Aurora Store.

- Open the Aurora Store App Accept terms of services.

- Next select Session Installer.

- Next select System Themes.

- Next select your preferred Accent.

- Next select Installer Permission.

- Toggle allow from this source to ON. and then click the back arrow and finish.

- Open the App Drawer (or the Home screen), long-press on Aurora Store, then tap the App info popover, which appears.

- Tap Permissions and move Files and Media from the NOT ALLOWED list to the ALLOWED list.

- Open Aurora Store.

- On the Welcome screen tap NEXT.

- On the Accounts screen tap ANONYMOUS. (NOT anonymous (insecure)). This will allow you to install apps without authenticating to the Play Store with a Google account of your own.

- As an exercise, click on any app you currently see in the Aurora Store.

- **DO NOT install.**

- Scroll down past the reviews.

There is a way to determine how many trackers and permissions are required for each App.

Click on the privacy arrow and to see what tracking information you are giving away to run the App.

Return, scroll down, to see what permissions will be required to run the App.

This is how you can help yourself make an informed decision on what you install. Always compare apps before installation.

~

Installing Brave browser
<mark>(INSTALLED)</mark>

Brave is a free and open-source web browser developed by Brave Software, Inc. based on the Chromium web browser. Brave is a privacy-focused browser, which automatically blocks online advertisements and website trackers in its default settings. There are several ways to download brave to your phone or PC, however, the less complicated suiting most users are as below;

- In Aurora store search Brave Private Web browser

- Click the default " Brave Software" icon which should appear at the top (not the beta or nightly)

- Click Install

- Click " Do you want to install this app" > Install > Open

- Untick " help improve brave by sending anonymous analysis"

- Set Brave as default browser if you wish

- Navigate to all apps (scroll up from settings to open App drawer) and open Brave browser.

- In the 3 vertital dots on the right-hand side click settings

- Click Search engines and change Standard tab to "startpage" or <mark>" brave"</mark>

- Return, and repeat for Private tab.

- Return to Home Screen and holding your finger on the default Vanadium Browser, drag it upwards to the "remove" tab.

- Return to the Apps page and drag the Brave Browser across and drop it into the vacated space.

- Hold your finger on the Brave browser icon for a second, open the info screen, navigate to the " Install unknown apps" and toggle ON.

~

Installing Signal (installed – Link your SIM to use)

Signal is a secure messaging app that can seamlessly manage all your messaging, both encrypted messages and conventional texts. It can also make encrypted voice calls. It's the best all-in-one messaging service for most users.

If a contact has Signal, they can receive your texts encrypted to their Signal account. If they do not have Signal, they will still receive the unencrypted message in their default message app.

- In a browser, browse to https://signal.org/android/apk/.
1.   **There is a shortcut on your desktop called 'Signal APK update' which you can use to download Signal updates when they are released instead of in app.

- Scroll down past the Danger zone heading and then tap the Download button.

- Tap Download in the Download file dialogue.

- Tap OK in the This type of file can harm your device notification.

- Once the Signal-website-universal-release…apk file has been downloaded, tap Open in the notification.

- *** Occasionally** it will not be seen that the download has finished and you will need to navigate back to the files/download folder in the main app page.

- Tap INSTALL in the Signal, Do you want to install this application? dialogue.

- Tap Done in the Signal App installed dialogue.

- Go to the newly installed Signal App Icon and press for a few seconds. Click on app info. Scroll down to Install Unknown apps and Toggle Allow from this source to ON.

- Signal needs this permission to be able to update itself.

- Once again, go to the newly installed Signal App Icon and press for a few seconds. Then tap the App info pop-over, which appears.

- Tap Permissions and allow Camera - Only while using this App, then Microphone- Only while using this App then individually Contacts, , Phone, SMS from the DENIED list to the ALLOWED list.

- Tap the back arrow at the top left of the screen.

- Tap Notifications and toggle Other to off.

When this setting is on, you'll see an icon reminding you that Signal is running in the background. The icon appears both on the lock screen and in the notification bar of the home screen. We find this icon distracting, so we prefer not to see it.

* If you prefer more automated updates to Signal, then it is recommended that you download the Signal app through Aurora Store instead of the APK file.

To Register and Configure Signal

- Put your SIM card into the phone. Signal needs this to register the new device.

- Open the Signal app and follow its setup/registration process. If you have a backup to restore, make sure you select the RESTORE BACKUP button when presented on the screen.

- After the registration step, Signal shows some action confirmations towards the top of the screen in white text on a blue background.

- Tap the use as default SMS app action confirmation, then select Signal in the dialogue that appears, and tap SET AS DEFAULT.

- Tap the Import system SMS action confirmation.

- Tap the x in the top right corner of the Invite your friends! action confirmation.

- Tap the Optimize for missing Play Services action confirmation, then tap ALLOW in the Let app always run the background? Dialogue.

~

Installing Proton Mail

Click here to install Proton Mail app directly from their APK:

https://proton.me/download/MailAndroid/ProtonMail-Android.apk

Follow prompts and add to your home screen once installed. It is strongly recommended to lock the app with a PIN code of its own (unique from your phone PIN) to further protect your account, and act as 2FA (Two Factor Authentication) on your mobile device.

This is done from the Settings menu in the Proton Mail app itself under Security.

Installing Telegram

Telegram is one of the most popular messaging services in the world and is focused on speed and security. Its core functionality is the same as most other messaging apps. You can message other Telegram users, create group conversations, call contacts, make video calls, and send files and stickers.

There are several ways of installing Telegram onto your phone. You can choose directly from their website at telegram.org, from the Aurora Store, or via F-Droid. **We highly recommend using the F-Droid 'FOSS' version, as it eliminates trackers present in the other versions.**

The F-Droid version is an unofficial fork that removes any proprietary dependencies, like:

- GSF (Google Services Framework), so it doesn't depend on Google for notifications.
- Google Vision face detection and barcode scanning (Passport)
- Google Wallet and Android Pay integration
- Google Voice integration and replaces some aspects with FOSS equivalents
- Location sharing with OpenStreetMap (osmdroid) instead of Google Maps

- Google Play Services GCM replaced with Telegram's push service

Play Store and website versions are provided by Telegram itself, and the website version has fewer regional content restrictions.

So if you have a de-Googled phone, you should really go with the F-Droid version.

- In F-Droid, find and install Telegram FOSS
- This will install, and the app icon will load to the home page.
- Press the icon for a second, then follow the Notifications button for an explanation of how the push notification works

~

Installing Maps with ==Magic Earth, Organic Maps== & OsmAnd

We find the best map solutions is from using two separate apps. The main drawback to this approach is the storage they take. Currently, we cannot go past OsmAnd~ as an offline maps and navigation app that depends on Satellite for navigation, and Magic Earth for City/urban directions. **Magic Earth** is my top recommendation to start with if you only pick one. Download the maps in the areas you need (state/country) for offline use, works very well with or without cell service if you have maps downloaded to the phone.
Organic Maps is our second app which is fully open source, however requires a Text to Speech (TTS) app for the voice commands to work. Just like with Magic Earth and OsmAnd, you can download a state/country for offline use later.

==*Magic Earth and Organic Maps have the state that we ship to downloaded, you may wish to download other areas or even the entire US. This allows for offline use of the map apps.==

You can dictate how much information you want to download. For example, if you want true contour lines and elevations in OsmAnd, add-ins are available. Your price is storage.

We use OsmAnd App for mountain biking, hunting, or hiking in remote areas, and for general area searching before visiting, to get a lay of the land.

As far as City work and driving, it gets us around but doesn't really drill down to the actual street numbers. For that reason, we use Magic Earth in urban environments, most people will find this the best and easiest option to replace Google Maps. If you don't rely on voice commands, Organic Maps is also an excellent choice.

This free App features the necessities such as lane assistance, turn-by-turn navigation, 2D, 3D, and satellite map views, route planning, the ability to use your phone as a dashcam, notification about speed cameras, and current speed limits. There are many more positives too that can be seen at their website www.magicearth.com.

To Install OsmAnd~

- In F-Droid, find and install Maps & GPS Navigation OsmAnd+ (known as OsmAnd~).

- After Install..Open

- Click Get Started.

- If you do not have a location available by default, Open the App Drawer (or it may be on your Home screen), long-press on OsmAnd~, and tap the App info popover.

- Tap Permissions and move location from the DENIED list to the ALLOWED list. Choose Only while the App is in use.

- Open OsmAnd~.

- Tap the period.

- Tap SKIP on the Download map screen, then tap SELECT in the Skip downloading maps dialogue.

- On the Map screens that follow, keep selecting your location as the options become more specific.

- When you see a Standard map option, tap it.

- This will download a map for your area. OsmAnd~ is an offline tool, so it needs to download maps of regions in which it will be used.

- In the World overview map notification, which appears next, tap DOWNLOAD.

- When fully installed, navigate to the App icon, press for a second, open the info dialogue, scroll down, and enable Location, "Only allow while using this App"

To Install Magic Earth <mark>(INSTALLED)</mark>

- In Aurora Store find Magic Earth Navigation & Maps

- Click Install

- Open, then at the bottom of the screen, at the download arrow, click, then search for 'United States' (or wherever you need to use the map)

- <mark>Download either the country, or the States and Territories you want to navigate</mark> (it may be in excess of 1Gb, so go make a coffee) for offline use if desired.

- After installation you will need to go to the Apps page (place your finger above the setting icon on the home page and scroll up) and drag it to the home screen.

- Press the icon for a second, then open the info bubble. Scroll down to location and allow "Only while using this app"

<mark>To install Organic Maps (INSTALLED)</mark>

- In F-Droid find Organic Maps

- Click Install

- Open, then in Settings you can select Downloaded Maps and click the plus sign in bottom right to add more maps to your device

- Add to Home Screen if desired

- Scroll through Settings to adjust anything desired

- *For voice commands to work, you must install a TTS engine (Text to Speech) from F-Droid*

~

Installing a Weather App

You can either choose to install a privacy-friendly weather app from F-droid, or create a browser shortcut to a local website where you can enter your location data.

As a rule, weather apps just repackage data from national weather services. So it makes more sense to have a shortcut rather than installing a weather app. This way, we can go straight to the source and keep it simple by adding a shortcut to the relevant weather service on the home screen.

- In Brave, browse to your national weather service forecast page for your city or region.
- Tap the 3 vertical dots icon in the bottom right corner of the screen and select Add to Home screen.
- In the Add to Home Screen dialogue, enter Weather and then tap Add.
- In the Add to Home Screen confirmation dialogue, tap ADD AUTOMATICALLY.

If you prefer to have a weather app, in F-Droid, search for Weather (Privacy Friendly) and install

~

Other Apps to Install from F-Droid and Aurora

We'll also install some other apps using F-Droid to provide various functionality. Search for each one by name in F-Droid, then install it. After installing each App, open it and approve the permissions it requests.

- **AntennaPod (INSTALLED)**- an open-source pod-cast manger and player

- **Blokada 6 or older version 5 (free)** – Alternative to a VPN, this is an excellent Ad-Blocker to view all incoming and outgoing connections. Cannot be used concurrently with another VPN, choose only one of these at a time.

- **Briar** messaging app – very anonymous and secure text message communication app.

- **Carnet**- a powerful note-taking app with many similarities to Google Keep. Not only writes shopping but also longer texts, stories etc.

- **Collabora Office**can be downloaded from Aurora Store It allows you to read and edit Microsoft Office (Word, Excel, PowerPoint) and LibreOffice documents directly on your phone or cloud service.
- **Element (Matrix)** – **Element.io** app offers an excellent free and open source communication app with endless features, and zero metadata tracking or collection, for both mobile and desktop systems.

- **Librera reader** highly customisable and feature rich application for reading e-books in a multitude of formats.

- **JitsiMeet (INSTALLED)**- An instant video calling and conference application for family, teams, or friends.

- **KeePassDX** an open-source, ad-free, multi-format password manager requiring no internet connection. (This is the companion to KeePassXC, an excellent password manager app)

- **K-9 Mail** can be downloaded from F-Droid, Aurora Store and Google Play Store. It is designed for both novice and power users, offering features like push notifications for IMAP and POP accounts, a unified inbox, themes, attachment saving, signatures, per account notifications, and emoji support.

- **MusicPiped** can be downloaded from F-Droid. It is a full-featured music player that streams from YouTube instead of playing local files. You can stream any music available on YouTube for free. It does not stream video and only fetches audio files, thus eliminating heavy data usage. It's a fully featured music player so you can enjoy background playback with notification controls, and you don't need to keep screen on and focused to listen to your music.

- **NetGuard** – app to view and block connections to your device, similar to Blokada

- **NewPipe**- has been created to get the original YouTube experience on your smartphone without annoying ads and questionable permissions. It offers many features that the YouTube app does not provide, like the option to download video or audio, a popup player, a background player, bookmarks, and play history – all without needing a Google account or having to log in.

- **Odysee** - a free and open-source video player and library across a variety of genres.

- **Session** – this is an up and coming private messenger app, very similar to Signal, but no number or email address is required, making this more anonymous. Video calling feature is coming soon, which will make this identical to Signal app.

- **Fossify Calendar Pro**- fully customizable, offline calendar with sync capability with no ads, complicated features, or unnecessary permissions.

- **Fossify Gallery Pro**- Off-line Photo and video gallery. The same version, but paid can be downloaded from Google Play Store. Browse, organize, edit, crop photos or videos, and recover deleted files from the recycle bin.

- **Fossify Voice Recorder (INSTALLED)**-is an easy way of recording any discussion or sounds without ads or internet access.

- **Standard Notes** is my recommended note taking app, free version is usually enough. This allows you to sync your Standard Notes to any devices you use, to work on projects and keep notes from any of your devices, right where you left off.

- **Session**- This is an excellent messenger app alternative to Signal, it is completely anonymous without the need to sign up with any true information at all.

- **Tasks.org** can be downloaded from F-Droid, Aurora Store, and the Google Play Store. It is free, open-source software based on the original source code from the popular Astrid Tasks & To-Do **Lists App**. Tasks can be used entirely offline or synchronized with Google Tasks, CalDAV, or EteSync.

- **VLC- (INSTALLED)** is a video and music player which just works! Regarded as one of the best FOSS Media players currently in the market supporting a wide range of formats for both local and remote playback.

- **Wire** – excellent messenger app similar to Signal, but only requires email to sign up, rather than a cell number making this more anonymous if desired.

~

Step 5 - Removing Unused Apps from the App Screen

Some apps bundled with GrapeheneOS are unlikely to be used often, and others we have replaced so we'll remove them from the App Screen to keep it as uncluttered as possible. This does not remove the programs from the phone, but only from our screen.

One is Auditor, which verifies the integrity of the operating system. Others include Gallery, PDF Viewer, and Vanadium.

- Open the App Page (put your finger near the settings icon and swipe up).

- Long-press on Auditor, then tap the App info popover which appears.

- Tap FORCE STOP, then tap OK in the confirmation dialogue.

- Tap DISABLE, then tap DISABLE APP in the confirmation dialogue.

- Repeat this process for Gallery (the black and white icon) PDF Viewer, and Vanadium browser
-

Now that vanadium has been removed from our phone we need to replace it with the brave browser for access. Hold the Brave browser icon with your finger and drag it down to the bottom of the screen, and release.

Now rearrange the home screen to your liking, and group like apps together.

~

Step 6 - Adjusting the Clock

We want the clock application to work with

- Open the App Drawer and tap the Clock icon.

- Tap the 3 vertical dots icon in the top right corner of the screen and select Settings.

- Tap Gradually increase volume and choose 30 seconds.

- This provides a less jarring experience when waking up to an alarm.

- Tap Start week on select Sunday, or whichever day you prefer.

~

Step 7 - Enhancing Jitsi Meet

- Open the App Drawer and tap the Jitsi Meet icon.

- Tap the 3 horizontal lines icon in the top left corner of the screen and select Settings.

- Type your first name or nickname into the Display name field.

- This identifies you in a call.

- Toggle Start with audio muted to on.

- If you leave this set to off, sooner or later, you'll find yourself in an awkward situation.

- Toggle Start with video muted to on.

- The same awkwardness could happen here as well.

~

Step 8 - Setting up Seedvault Backups

* SeedVault is currently experiencing some bugs and may not work properly. You can still backup your device to a computer or thumb drive, however you may get annoying notifications with some sort of error message about backups. GrapheneOS developers are aware of this issue and are working on a more stable option.

SeedVault is an encrypted backup app that is bundled with GrapheneOS. For this step, you'll need a USB flash drive (with a USB-C adapter) to be the target for the backup. Ideally, it will be at least the same size as your phone's storage, your phones are all 128Gb size for storage. This will provide you with a recovery drive essentially (minus the shared data as outlined in the next section) so keep this USB drive backup of your device in a safe place. Note that some apps such as Signal, due to their security protocols, will not display past messages, only current and ongoing on the new device that you install the recovery file onto. However all of your contacts and other app data will be present.

The data which Seedvault backs up doesn't include your phone's shared storage. Backups for that will be handled in the next step.

- Go to Settings > System > Backup.

- A 12-word recovery code is displayed. Record it somewhere secure.

- Tap the CONFIRM CODE button.

- Enter the recovery code and tap the DONE button.

- Plug the flash drive into the phone.

- Tap CANCEL in the F-Droid > Open F-Droid to handle…dialogue.

- Tap your flash drive's name on the Choose where to store backups screen.

- Toggle Back up my data to ON on the Backup screen.

- Tap the 3 vertical dots icon in the top right corner of the screen and select backup now to run your first backup.

~

Step 9 - Setting Up Shared Storage Backups

Because Seedvault doesn't back up the phone's shared storage, we need to back up shared storage in a separate step. We recommend backing it up to a second flash drive which is fully encrypted.

- Plug the flash drive into your computer, then mount and unlock it.

- Connect the phone to the computer.

- Copy the phone's shared storage to the flash drive.

It may not be necessary to do this right now, as you've just set your phone up and the amount of data in shared storage is probably minimal. This is a procedure you should carry out regularly from now on though based on your need for frequency.

Also a good check once your phone is setup initially, disable OEM unlocking, and disable Developer Mode in your Settings menu unless you need those for something specific. This aids in maintaining best security practices while using your new device. Enjoy and please reach out with any questions or if you have anything you can add to better update and understand GrapheneOS.

~

That should get you going, for more support, please email us at phones@graphenegoat.com or at Proton Mail for encrypted messages, graphenegoat@protonmail.com, or visit https://grapheneos.org/ website or support forums for more information. Our website https://graphenegoat.com has a ton of resources also to look through. Thank you again, we look forward to assisting you with your new de-Googled GrapheneOS phone, these are the most privacy respecting mobile devices currently available.

-GrapheneGoat

https://graphenegoat.com