#BoycottBigTech

MARK37.COM

MARK37 Ghost Phone
Getting Started Guide

This comprehensive guide is designed to facilitate your initial setup and familiarization with your newly acquired secure communication device. We strongly advise reviewing this guide in its entirety, as it offers indispensable instructions, valuable tips, and a comprehensive overview of utilizing your phone effectively.

The Device

Our phones come equipped with GrapheneOS, an Android-based operating system that prioritizes privacy, security, and open-source principles. With GrapheneOS, your device is protected against tracking and spying attempts from large technology companies and other third parties.

This guide will walk you through the initial setup and configuration of your phone in a step-by-step manner. If you encounter any difficulties or have questions, please don't hesitate to contact our support team at support@mark37.com.

Alternative App Stores

When using a de-Googled phone, you may need to find alternative apps that work without relying on Google services. Here are a few ways to discover such apps:

F-Droid: F-Droid is an open-source app store that hosts a collection of free and open-source apps. It provides a wide range of apps that do not depend on Google services. You can visit the F-Droid website (https://f-droid.org/) and explore the available categories to find alternatives to popular apps.

Alternative App Stores: Besides F-Droid, there are other alternative app stores that offer non-Google apps. For example, Aurora Store is a third-party client for the Google Play Store that allows you to download apps without needing Google Play Services. You can also look for alternative app stores like APKMirror, APKPure, or Aptoide. However, be cautious when downloading apps from third-party sources and ensure they come from trusted and verified providers.

Privacy-Focused Websites and Communities: Several websites and communities focus on privacy and provide recommendations for de-Googled apps. Privacy-oriented websites like PrivacyTools (https://www.privacytools.io/) often provide curated lists of privacy-friendly apps across different categories. Additionally, online forums, subreddits (such as r/privacy), or online communities dedicated to de-googling may have discussions and recommendations for alternative apps.

Research and Online Reviews: Conduct online research and read reviews or articles about de-Googling your phone. Many privacy-focused tech websites and blogs often review and recommend alternative apps that work well on de-Googled devices. Look for articles specifically discussing de-Googled phones or privacy-conscious app recommendations.

Remember, when replacing apps, it's essential to consider your specific needs and preferences. Some apps may offer similar functionality but with different interfaces or features. It may require some experimentation and trial to find the apps that best suit your requirements on a de-Googled phone.

On Startup

To ensure a smooth start with your de-Googled phone, follow these step-by-step instructions:

1. Power on your phone by pressing the small colored button located on the right side of the frame for 2 or 3 seconds. You will see a warning message stating, "Your device is loading a different operating system." This is normal and will appear each time you start or restart the device. Simply leave the phone untouched, and it will progress to the next screen automatically.

2. The Google logo will appear during the bootloader process. Please note that you are not installing any Google software on the phone. Treat it in the same way you see the Dell or HP logo when starting your laptop or desktop. We can happily ignore the Google logo.

3. Next, the GrapheneOS start screen will appear, indicating that your phone has undergone the basic setup process. However, we recommend adjusting the settings to your preferences by following these steps:

    - **Language**: Set the language to your country and preferred language. The default is English (United States). To do this, go to **Settings > System > Languages & input > Languages** & press "**add language**".

    - **Time and Date**: Set the time zone, date, and time according to your location. Initially, your phone is set to Eastern Time, so please adjust it as needed. Access the settings by going to **Settings > System > Date & time**. To set the default time zone, toggle off "**Set time zone automatically**". If you want your phone to update date and time zones automatically while traveling, make sure to toggle on "**Set time zone automatically**".

    - **Wi-Fi**: Connect to an available Wi-Fi network. Swipe down from the top of the screen and tap on "**Internet**." The list of available networks will be displayed automatically. Tap on your network to connect to it. You will be prompted to enter your Wi-Fi network password. Enter it and press "**Connect**".

By following these steps, you will ensure that your de-googled phone is set up correctly and ready for use.

Special Notes:

1. **Wi-Fi**: When you power on your de-googled phone, the Wi-Fi will automatically toggle on. If it's turned on, the phone will connect to known Wi-Fi networks such as your home or workplace. If it's turned off, you will need to manually connect to a Wi-Fi network. We recommend keeping the toggle off to avoid automatically joining networks unless desired.

2. **VPN and Wi-Fi Scanning**: Enabling the Wi-Fi toggle will also activate Wi-Fi scanning, which means your phone will constantly search for Wi-Fi networks. This may not be preferable for everyone, especially considering privacy concerns. While a reliable VPN can provide protection, it's important to be aware of the implications of turning on Wi-Fi scanning.

3. **Inserting SIM Card**: If you have access to Wi-Fi during the setup process, you can skip inserting a

SIM card. However, if you want to use cellular data for setup or ongoing usage, you will need to insert a SIM card. If it's a new SIM, you may be required to register with your service provider. Note that charges may apply depending on your data usage.

4. **Location Services**: During GrapheneOS setup, you can decide if you want apps to have automatic access to your location. By default, we disable this global location setting and recommend modifying permissions on an app-by-app basis. You will need to toggle on location for any app that requires it. This ensures that your phone's location remains off unless explicitly enabled or granted permission by specific apps.

5. **Secure Your Phone**: It's crucial to set up security features to protect your phone from unauthorized access. You can choose from options such as fingerprint or face recognition (if supported by your phone model), PIN, and/or password. We recommend setting up at least one of these security features. Upon delivery, these features will be deactivated, so please refer to the instructions further in the manual to activate and configure them.

6. **PIN Scrambling**: GrapheneOS offers built-in security features, including PIN scrambling. This feature randomly rearranges the position of numerals on the keypad each time you log in, enhancing security by preventing others from guessing your PIN by observing your keystrokes. To enable PIN scrambling, go to **Settings > Security > Scramble PIN input layout** and toggle it on.

By following these additional steps, you will ensure a more secure and personalized setup for your de-Googled phone powered by GrapheneOS.

Initial use of GrapheneOS

Customizing How You Navigate:

By default, your de-Googled Ghost phone has been setup to leverage the “3 Button Navigation” system. If you prefer to go back to the swipe navigation system, you can change it. To do this, go to **Settings > System > Gestures > System navigation**. You can also find this option in **Settings > Accessibility > System controls > System navigation**.

Gesture Navigation:

- To go to the Home screen, swipe up from the bottom of the screen and remove your finger.
- To access recently used apps, swipe up from the bottom of the screen and hold your finger for a moment before releasing.
- The most recently opened app is always on the right side. Swiping to the left takes you back through your recently used apps.
- To go back within an app, swipe from the left or right edge of the screen towards the center.
- To navigate between recent apps without changing their order, swipe left on the navigation bar for the previous app and swipe right for the next app.
- To open the app drawer, swipe up from anywhere on the screen (except the navigation bar).

3-Button Navigation:

- This navigation style uses three buttons at the bottom of the screen: Back (left), Home (center), and Recent Apps (right).
- The most recently used app is on the right side in the recent apps list. Swiping to the left goes back through your app history.

***System Tweaks*:**

***Network and Internet*:**

- If you have limited data, go to **Settings > Network & Internet > Data Saver** and toggle it on. Only use this if necessary, as it may slow down some apps.

***Battery*:**

- We have already adjusted the phone to display the battery percentage in the notification bar. To change this, go to **Settings > Battery** and toggle off "**Battery Percentage**."

***Sound*:**

- Adjust the ring and notification volume by going to **Settings > Ring and notification volume** and setting it to half.

***Display*:**

- To make viewing easier, go to **Settings > Display > Adaptive brightness** and toggle it on.
- For privacy, go to **Settings > Display > Lock screen > Privacy** and select "**Don't show notifications at all**."
- To check the phone, tap the power button instead of tapping the screen. Go to **Settings > Display > Lock screen > Tap** to check phone and toggle it off.
- To show a double line clock on the lock screen, go to **Settings > Display > Lock screen > Double Line Clock** and toggle it on.
- To avoid accidental wake-ups, go to **Settings > Display > Lock screen > Lift** to check phone and toggle it off.
- To minimize distractions, go to **Settings > Display > Lock screen > Wake screen for notifications** and toggle it off.
- Set the screen timeout to 2 minutes in **Settings > Display > Screen timeout.**
- To reduce eye strain, go to **Settings > Display > Night Light** and toggle it on. Customize the schedule instead of using sunrise and sunset times.
- Enable auto-rotate screen in **Settings > Display > Auto-rotate screen**.
- If you're using a thick screen protector, go to **Settings > Display > Increase touch sensitivity** and toggle it on.
- To customize the on-screen keyboard, go to **Settings > System > Languages & input > On-screen keyboard > GrapheneOS keyboard**. Select English (US), turn off "**Vibrate on keypress**," choose the "**Material Dark**" theme, and enable personalized suggestions.

***Security*:**

- **Settings > Security > Screen lock**: Set your preferred login PIN/Password.
- **Settings > Security > PIN scrambling**: Toggle it on.
- **Settings > Security > Screen lock camera access**: Toggle it off.

Remember to secure your phone with a PIN, Fingerprint, or Password to protect against physical exploitation.

Installing Apps on Your De-Googled Phone

When it comes to installing apps on your de-Googled phone, there are multiple options: Reckless, Careful, and Cautious. To ensure maximum privacy and security, we recommend taking the cautious approach.

Reckless Option:
The reckless option involves quickly downloading apps from the Google Play store and then deleting your Google account. However, this approach may still leave traces of Google services and compromise your privacy.

Careful Option

The careful option is to set up another account on your phone, creating a "sandboxed" environment. Think of it as a quarantine ward for apps, isolated from the rest of your phone. This account will only contain apps that are potentially harmful to your privacy. Be cautious when using this option and ensure that you only install trusted apps.

Cautious Option

The cautious option is to use the Aurora Store, an open-source client for the Google Play Store. It allows you to search, download, and update Android apps and games without relying on Google services. To install apps via Aurora Store, follow these steps:

- Download the Aurora Store app (already installed on your phone).
- Open the Aurora Store app.
- Use the search function to find the app you want to install.
- Select the app from the search results.
- Click the "Install" button to download and install the app on your phone.
- By choosing the cautious option and utilizing the Aurora Store, you can carefully select and install apps while maintaining your privacy and security. Remember to only install apps from trusted sources and regularly update them to ensure they remain secure.

Safest Option

For the utmost privacy and security, we recommend using the F-Droid Store to install apps on your de-googled phone. F-Droid is a trusted repository of free and open-source (FOSS) apps, which prioritize user privacy and have minimal permissions. By using apps from F-Droid, you can enjoy a high level of assurance that your data is protected and your privacy is respected.

To access and install apps from the F-Droid Store:

1. Open a web browser on your de-Googled phone.
2. Visit the F-Droid website by typing in www.f-droid.org.
3. On the F-Droid website, you can browse through the available apps or use the search function to find specific apps.
4. Click on an app to view more details about it, such as its description, user ratings, and reviews.
5. If the app meets your requirements, look for the "Download APK" or similar button on the app's page and click on it.
6. Once the APK file is downloaded, open the file to begin the installation process.
7. Follow the on-screen instructions to complete the installation of the app.
8. Once installed, you can find the app on your phone's app drawer or home screen, ready to be used.

By using the F-Droid Store, you can have peace of mind knowing that the apps you install are free from trackers and respect your privacy. The FOSS nature of these apps ensures transparency and allows security experts to review the code for any potential vulnerabilities.

Remember to regularly update your apps from the F-Droid Store to benefit from the latest features and security improvements.

Using the F-Droid Store as your primary source for app installations on your de-Googled phone offers a secure and privacy-focused experience while enjoying a wide range of free and open-source applications.

Another safe option – App-like links to web applications and websites

If you come across a website or web application that you frequently use and want quick access to, there's an alternative to installing a dedicated app. Instead of downloading an app from the website, which may redirect you back to Google and compromise your privacy, you can create an app-like shortcut icon on your phone's screen.

Here's how you can create a shortcut icon for a website or web application:

1. Open the web browser on your phone.
2. Go to the website or web application you want to create a shortcut for.
3. Once you're on the desired page, tap the browser's menu or options button (usually represented by three dots or lines) to open the browser's settings.
4. Look for an option like "Add to Home Screen" or "Create Shortcut." The wording may vary depending on the browser you're using.
5. Tap on the option to create the shortcut.
6. A prompt will appear asking you to confirm the creation of the shortcut. You can usually customize the name of the shortcut at this stage.
7. Tap "Add" or "Create" to finalize the process.
8. The shortcut icon will now be added to your phone's home screen or app drawer, depending on your device and launcher.

By creating these app-like shortcuts, you can access websites or web applications directly without the need to download and install a dedicated app. It provides a convenient way to reach your favorite sites while maintaining your privacy and avoiding unnecessary data collection.

Just remember that these shortcuts are essentially links to websites, so they may not offer the same level of functionality as dedicated apps. However, they can be a great alternative for websites that you frequently visit and want quick access to without compromising your privacy.

Internet & Browser

For best privacy and security, it's important to consider the following components: DNS servers, web browsers, and search engines. While they may seem separate, they are interconnected, and the choices we make in these areas can greatly impact our privacy. To fully benefit from using a de-Googled phone, it's crucial to make the right decisions in these aspects.

1. DNS Servers:
   DNS (Domain Name System) servers are responsible for translating website addresses into IP addresses. By default, your phone uses DNS servers provided by your internet service provider (ISP), which may compromise your privacy. To enhance privacy, you can consider using alternative DNS servers that prioritize security and do not log your browsing activity.

2. Web Browsers:
   Web browsers are the apps you use to access websites. While popular browsers like Chrome or Safari may come pre-installed on your phone, they are often associated with data collection and tracking. Opting for privacy-focused web browsers can help protect your online activities. These browsers are designed to block trackers, minimize data collection, and provide additional privacy features.

3. Search Engines:
   Search engines are the tools we use to search for information online. Most popular search engines collect and store user data to deliver personalized results and targeted ads. However, there are privacy-focused search engines available that prioritize user privacy by not tracking or storing your search history. Using these search engines can enhance your privacy and reduce data collection.

By making informed decisions about DNS servers, web browsers, and search engines, you can maximize the privacy and security benefits of using a de-Googled phone. It's essential to choose options that prioritize privacy, minimize data collection, and provide enhanced security features.

Ad-Blocking

Ads can be annoying, like bothersome flies that distract you while you're reading. They seem to keep coming back no matter how many times you try to get rid of them.

To block ads, you have three main options: a private DNS service, a paid or free ad-blocker extension, or an ad-blocking browser. However, since we'll be using apps from F-droid, which is focused on privacy, we won't encounter as many problems with ads compared to the regular Google Play Store. This means there will be less ad tracking and fewer intrusive ads.

Private DNS Service

A DNS (Domain Name Server) is like the postman of the Internet. It takes the website names we type in and translates them into IP addresses, which are like GPS coordinates for websites. By default, your network provider gives you a DNS server, but they may log your browsing history and sell it to third parties. You can override this and choose a private DNS server that prioritizes privacy, such as DNS ad-guard. However, using a private DNS server might make you stand out and be more easily identified, so it's a trade-off between privacy and blending in.

To set up a private DNS, go to **Settings > Network and Internet > Private DNS > Private DNS provider hostname** and enter your server's name (e.g., dns.ad-guard.com).

Ad-blocking Extension

GrapheneOS, the operating system we're using, comes with a secure browser called Vanadium. It's recommended not to add ad-blocker extensions to the browser or modify the default settings, as it can make you more trackable. The focus of Vanadium is on security rather than ad-blocking. Therefore, installing an ad-blocking extension on the default browser is not necessary for our purposes.

Ad-blocking Browser

GrapheneOS recommends using Bromite, a Chromium-based browser, as an alternative to Vanadium. Bromite has integrated ad-blocking and advanced anti-fingerprinting features. It is designed to provide a combination of the best features for privacy and security while browsing the web. You can install Bromite as your ad-blocking browser instead of using the default browser.

Considering our options, installing a private DNS service or using an ad-blocking browser like Bromite can effectively block ads. However, since we'll be using F-droid apps with fewer ads, the impact of ads will already be reduced.

Additionally, let's not forget about VPNs (Virtual Private Networks). A VPN encrypts your network traffic and masks your IP address, providing an extra layer of anonymity. It helps protect your data from your internet provider and makes it harder for them to track your browsing history. Some VPNs also include ad-blocking features.

If you're interested in using a VPN, it's important to choose a reliable provider. We recommend VPN services like ProtonVPN and CalyxVPN, which have a strict no-logging policy and are known for their commitment to privacy. Another option is to set up your own self-hosted VPN, although that requires more technical knowledge.

Remember, ad-blocking and VPNs can enhance your privacy and security while browsing the web. Choose the method that best suits your needs and preferences, keeping in mind the trade-offs and benefits of each option.

Internet & Browser Recommendation

Based on the information provided, our recommendation is to use an ad-blocking browser along with a VPN to ensure a high level of privacy, an ad-free experience, and reasonable anonymity.

One recommended browser is Brave, which not only blocks ads but also incorporates private search engines. Brave browser, along with Vanadium, is my preferred choice most of the time.

Privacy Browser (available from F-Droid), is another option that utilizes the Mojeek search engine. Mojeek provides unbiased search results compared to Google.

Startpage is another tested and reliable search engine that prioritizes privacy and returns decent results. Startpage anonymizes search requests and doesn't store any data, such as search queries or IP addresses. They are based in the Netherlands, and any requests for information would need to come from Dutch judicial authorities. However, it's important to note that Startpage uses Google (anonymously) as the search engine, so the results may still be influenced by Google's algorithms.

By using an ad-blocking browser, such as Brave or Vanadium, along with a VPN, you can enhance your privacy, block ads, and maintain a certain level of anonymity. Additionally, consider the search engine options mentioned, such as Brave search engine, Mojeek, or Startpage, for more private and unbiased search results.

To ensure a privacy-focused and secure browsing experience on your de-Googled phone, follow these steps:

1. Keep the default DNS settings and ensure they are not modified.
2. Install the Brave browser as your default browser if you prefer enhanced privacy features and built-in ad-blocking.
    - Go to the app store on your de-Googled phone.
    - Search for "Brave browser" and install it.
3. If you prefer to stick with the default Vanadium browser, follow these steps to set it up:
    - Open the Vanadium browser on your de-Googled phone.
    - Access the browser settings.
    - Navigate to the privacy and security options.
    - Enable privacy features like blocking third-party cookies, disabling JavaScript, or enabling the Do Not Track option.
    - Configure the search engine preferences to use more private and unbiased options like Mojeek or Startpage.
    - Customize other browser settings according to your preferences.
4. Grant Vanadium permission to install unknown apps.
    - Go to the Home page of your de-Googled phone.
    - Locate the APP Quick Access bar at the bottom of the page.
    - Press and hold the Browser Icon (tri-colour circle icon) for a few seconds.
    - Click the information icon that appears.
    - Scroll down and enable the "Allow from this source" toggle to ON.

Once you have set up your preferred browser (either Brave or Vanadium), you can proceed to download and install the necessary services and apps for a comprehensive privacy experience:

- F-Droid: Go to the F-Droid website (www.f-droid.org) on your browser and download the F-Droid app.
- VPN: Choose a VPN service provider that aligns with your privacy requirements. Install their VPN app from the app store or directly from their website. We highly recommend MulvadVPN,
- Aurora Store: Go to the Aurora Store website (auroraoss.com) on your browser and download the Aurora Store app.
- Brave browser (if using Vanadium): Open the Vanadium browser and visit the Brave website (brave.com). Download and install the Brave browser app.

Following these steps will help you establish a privacy-focused and secure browsing environment on your de-Googled phone, allowing you to enjoy a safer online experience.

VPN Services

Mullvad VPN Service: Our #1 recommended VPN

To install the Mullvad VPN, it's recommended to choose a server location that is relatively nearby to ensure better internet speeds, unless you have a specific reason to use a server in another country.

1. Upon opening the app, you may need to create a Mullvad account. Look for the "Create account" option at the bottom of the screen and follow the instructions to set up your account.
2. Take note of your Mullvad account number as you will need it later.
3. To use the Mullvad VPN service, you need to purchase credit for the desired time and payment method. Look for the "Buy Credit" option within the app and follow the prompts to make your purchase.
4. Once you have credit, you can select a server location. It is recommended to choose a server from a nearby location to ensure better internet speeds. Select your preferred country from the available options.
5. After selecting a server, tap "OK" to establish a connection with the VPN.
6. Wait for the "Secure Connection" notification, which confirms that your connection is encrypted and secure. The notification will also indicate the city you are connected to.
7. If you wish to customize your Mullvad VPN settings, tap on the Settings icon (usually represented by three vertical dots) at the top right of the screen. From there, you can access preferences and adjust settings according to your preferences.
8. To ensure a consistent VPN connection, you can enable the "Auto-connect" option in the app's preferences. This will automatically connect you to the VPN whenever you use your device.
9. For added security, you can enable the "Always-on VPN" and "Block connections without VPN" options in your phone's settings. To do this, go to your phone's Settings, navigate to "Network and Internet," then select "VPN." Find the Mullvad VPN in the list of installed VPNs and toggle the "Always-on VPN" and "Block connections without VPN" options to the "ON" position.
10. To avoid receiving notifications about the VPN status, you can disable notifications specifically for the Mullvad VPN app. Go to your phone's Settings, select "Apps" or "Applications," then choose "All apps." Locate the Mullvad VPN app in the list and tap on it. Look for the "Notifications" option and toggle it to the "OFF" position.

Aurora Store - The Private and Secure Alternative to Google Play Store

The Aurora Store is a powerful and privacy-focused client for the Google Play Store, designed to provide users with an alternative way to download and update Android apps. It functions similarly to the official Google Play Store but offers a significant advantage – it respects your privacy and allows you to use the Play Store anonymously.

Why You Should Use Aurora Store:

1. **Privacy Protection:** Unlike the Google Play Store, which collects extensive data about your app usage and device, Aurora Store removes many of the invasive trackers and permissions associated with Google services. When you use Aurora Store, your app installations and updates happen without exposing your identity to Google.

2. **Anonymous Access to Apps:** Aurora Store enables you to "log in" anonymously, spoofing your account details to protect your privacy. For instance, if you log in as "John Doe" once, the next time you log in, it will automatically generate a different account name like "Jane Doe," without ever revealing your real identity.

3. **Trackers and Permissions Transparency:** Aurora Store allows you to view the number of trackers and permissions required by each app before installation. This helps you make informed decisions about which apps you want to download, ensuring you understand the data they might access.

4. **F-Droid Integration:** Aurora Store can be easily installed from F-Droid, a trusted repository of free and open-source apps. This adds an extra layer of assurance for privacy-conscious users who prefer to obtain apps from trusted sources.

By using Aurora Store, you can protect your privacy, limit the tracking of your app usage, and gain more control over the permissions granted to apps on your Android device. It's an excellent choice for privacy-conscious users who seek a secure and private alternative to the official Google Play Store. Remember to compare apps before installing them, and enjoy a safer and more private app downloading experience with Aurora Store.

Brave Browser - A Privacy-Focused Web Browsing Solution

Brave is a secure and privacy-oriented web browser built on the Chromium platform by Brave Software, Inc. Unlike traditional browsers, Brave takes your online privacy seriously and comes with default settings that block online advertisements and website trackers automatically.

Setting Up Signal Secure Messaging App

Signal is a highly secure messaging app that allows you to manage both encrypted and conventional texts seamlessly. It even supports encrypted voice calls, making it an excellent all-in-one messaging service for most users. Here's how you can install and configure Signal on your device:

Registering and Configuring Signal:

1. Insert your SIM card into the phone; Signal needs this to register the new device.
2. Open the Signal app and follow the setup/registration process. If you have a backup to restore, select the "RESTORE BACKUP" button when prompted.
3. After registration, Signal will show some action confirmations. Tap "use as default SMS app," then select Signal in the dialogue and tap "SET AS DEFAULT."
4. Tap "Import system SMS" to import your existing SMS messages.
5. Tap the "x" in the top right corner of the "Invite your friends!" action confirmation.
6. Tap "Optimize for missing Play Services," then tap "ALLOW" in the "Let app always run in the background?" dialogue.

Congratulations! You now have Signal configured on your device, providing you with a secure and private messaging experience. Enjoy communicating with peace of mind knowing your messages are encrypted and protected.

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 FDroid '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.

NOTE: You will not be able to create a new Telegram account from the FOSS Telegram app that is pre-installed on your Ghost Phone. This will unfortunately need to be done from a device running the non-FOSS version of the app (laptop or your current Google Android or iPhone). You can also install sandboxed Google Play Services on your Ghost Phone, download the full Telegram app from Aurora, setup your account, activate your account from the FOSS version of the app, and then remove the full Telegram app and uninstall Google Play Services. See the very last section of this Guide for how to go about installing sandboxed Google Play Services on the device.

Maps with Magic Earth

Magic Earth is our top recommendation. 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.

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.

Apps Installed on Your Device

A complete list of the apps you have installed on your Ghost Phone, and what each of them does, can be found at → https://mark37.com/blog/current-apps-installed-on-the-ghost-phone/

As we sometimes update the apps installed, we've chosen to keep this list up to date in a single location via the link above.

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.

Adjusting the Clock

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 Home time zone and select your time zone.
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.

Setting up Seedvault Backups

(We consider this a high priority task once you start using your phone to prevent the loss of data **)**

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. 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.**
- Tap Recovery code and Generate new code at the bottom. Carefully record it somewhere secure.
- Tap the CONFIRM CODE button.
- Enter the recovery code and tap the DONE button.
  - **NOTE:** You should not have to Generate a new code for future back ups once you generate you first one. But if you do you will still need the previous code to recover back ups made using that code. So be sure to keep copies of all generated codes.

- 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.

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.

CAUTION AREA:

Device Tracking

Device tracking refers to the process of monitoring and recording the location and activities of a device, such as a mobile phone or GPS tracker. It involves using technologies like GPS (Global Positioning System) or RFID (Radio Frequency Identification) to determine the device's precise location and transmit that information to a receiver.

GPS tracking devices, for example, use satellite signals to calculate the device's location, time, and velocity. This information can be represented in three-dimensional views and used to track the device's movements. GPS systems consist of three segments: space, control, and user.

Cross-device tracking is another form of device tracking that involves linking multiple devices used by an individual to create a comprehensive profile. This allows companies to gather more data about a person's behavior and preferences across different devices. Cross-device tracking can be privacy-invasive, as it can reveal a complete picture of a person's activities and potentially compromise their privacy.

There are various tracking mechanisms and technologies used for device tracking, such as GPS receivers, RFID tags, barcodes, and even virtual tracking systems in virtual reality environments. These mechanisms collect and process location data, either in real-time or with a certain lag time, to provide a sequence of location information for further analysis.

It's important to be aware of device tracking and its implications for privacy. While tracking can have benefits, such as recovering lost items or optimizing fleet routes, it's crucial to understand how your device is being tracked and consider the potential privacy risks associated with it. Taking steps to manage permissions, using sandboxed accounts, and being cautious about granting access to personal data can help mitigate some of these risks.

Google Apps & Google Play Services

It is possible to install Google Apps & Google Play Services on your Ghost Phone, and GrapheneOS has made it simple to do so. However, we strongly recommend that you avoid installing Google Apps & Services on your Ghost Phone at all costs. Before doing so, we highly recommend that you consider all options and the actual necessity before proceeding. Ask yourself questions like, can it be done through a web browser, or is it just an inconvenience like not being able to do mobile check deposits?

If after careful consideration and looking at all options, you still must have Google Apps & Services on your phone, it can be done, and doing it with GrapheneOS is probably your safest option. GrapheneOS installs apps in sandbox environments, so all apps must be given permission to access anything outside that sandbox they run in. Google Apps & Services installs just like any other app, so it can be run quite securely and safely if you are extremely careful about your permission settings.

There are two ways to do this. The first and best option is to create a second user account in which you install Google Apps & Services and only run the apps needing such in this account. We call this a sandbox account. This will be the safest, most private way to use Google Apps & Services on your device. This way, if you ever were to accidentally give any apps using Google Apps & Services permission to access all of your files or any some access to other apps, you are not in danger of giving Google access to the private information stored on your phone but only to what information and data that is stored in this sandboxed user account. It is for this reason we suggest never storing pictures, files, or any other personal data you are not willing for big tech or anyone else to get their hands on inside this sandbox account.

The second option is to just install Google Apps & Services in your primary account. This is not very good or recommended at all, but still better than using a Google Phone. All apps in GrapheneOS are sandboxed to prevent cross-app tracking, so it does help with privacy and tracking, but only if you are very careful in managing your permission and never make a mistake. Installing Google Apps & Services in this account can be done fairly safely, but only if you are managing permissions properly. For this guide, we will only provide instructions here for installing Google Apps & Services in a sandbox account, which is the only way we recommend it be done.

Go to **Settings** > **System** > **Multiple users**.

In here toggle **Allow multiple users** to **ON**. Then tap **Add user**. You can read the pop-up and press **OK**. Next you will be given the option to add a profile photo and give the account a name. I suggest naming this account Sandbox but you can give it any creative name you wish.

The next screen gives you the ability to control how this account is used. Here you can choose what type of apps can be installed if any. You can disallow calls and SMS messaging here if you like also. I would allow installing apps as the purpose of this account is to install apps that you do not want in your primary user account. One thing we should do here is install The Aurora store. To do this click on **Available apps** and check Aurora Store. You may also check any other apps you wish to have installed. I would be very careful of installing any other apps as you are wanting to only use this account for apps requiring Google Apps & Services. Once you have made your choices press **Switch to New user**. Next tap **Set up now**.

The next steps are used for setting up the Account.

- Press **Start**
- Choose your language and press **Next**.
- I suggest leaving Location Services **unchecked** and only allowing location services as need in the account.

- Next set up your Finger print, Face ID or Pin. Depending on what want to use and your device's options.
  Once you are at Restore Apps press **skip**.
- Then press **Start** and you will be in the Sandbox account.

Now we can begin the process of installing Google Apps & Services.

Swipe Up from the bottom to display all the apps in you sandbox account. In the right top corner you should see an icon that looks like a box labeled **Apps**. Click on it. Then at the bottom of this page you will see **Google Play services**. Open this and you will see three items listed under **Dependencies**. We will install all three. To install the items press the button near the top that says **Install**. It will begin downloading the dependencies. After a moment a pop up will appear. Here will need to leave **Network permissions** checked and press **install**. Two more pops will appear after the first and you will do the same with them first pop up.

Once the installation is complete you can go to the home screen. You will see the Google Play store in your list off Apps now. But I suggest you do not use it but instead wish the Aurora Store for downloading your needed apps unanimously.

You can now safely download and use apps requiring Google Play services safely separated from you main account. You do need to be aware though that any data, personal info used in any app on this account can likely be accessed by Google and possible other third party entities that Google has partnerships with. Although these apps can not share data with each other this only prevents the apps themselves from sharing data with each other and the creator of those apps from seeing any data from others and any cross app tracking. Google still has a tunnel into each app that is using its services and any data, files or sensors you have given that app permission to access.

CONCLUSION

We hope this document as provided you with the information you need to started successfully using you Ghost Phone and to make informed decisions on operating your phone in a secure & private way. If you have any questions or need more support, please email us at support@protonmail.com, or visit https://forums.mark37.com/forum/all-about-ghost-phones-6/ to access our forums for more information.

Thank you again, we look forward to assisting you with your new de-Googled MARK37 phone!

~ The Team at MARK37.COM