A Sandbox on Your Phone. Here's How Apps Are Isolated

A major advantage of Mosaic OS is that you can manage more than just application permissions, but you can also specify the exact environment where each app and user profile should run. In this video, we demonstrate how profiles function, how to use them to keep work and personal life separate, and how to set up a secure environment for kids or guests, and why the source of your app downloads is important.

Using Profiles

Even when using one profile, Google apps operate in a sandbox, essentially giving them their own private playground, from which they cannot see outside or access any other activities taking place on your device. Applications that do not require Google Services to operate can be downloaded from sources like the Aurora Store. These are automatically placed in a so-called container and only have access to the functions for which the user grants permission. Applications are unable to view anything on your device unless you have explicitly given them permission, however, you should keep in mind that some applications and features need specific permissions to communicate.

Setting up separate user profiles offers even greater isolation. For instance, you could have a personal profile, a work profile, and even a separate financial account, where you isolate your banking applications. You can switch between these profiles with ease. If you just switch from one profile to another, the previous profile may still run in the background, so you can receive its notifications if you allow it. To do this, access **Select user** from the top of the home screen, **Manage users →Send notifications to current user** turned on. However, if you choose to exit by selecting the **End session** option from your profile, the session will be fully terminated, and you will stop receiving those notifications. This is particularly helpful if you want to keep your work and banking applications entirely separate from each other. Furthermore, you can configure it so that exiting an account always closes all sessions within it, just as if you had powered that account down. This option is only configurable from the main profile. **Select user →Manage users**. You will need to select the account you wish to apply this to, and then **Allow running in background** is switched off. Isolating profiles is also a great way to provide a secure environment for others, like your children. The **Guest profile** option lets you create a distinct space. You can create a new guest profile with the **Add guest** option. Here, among other things, you can control what options the guest can use, you can also restrict the ability to install and update applications. Furthermore, you can turn on the **Delete guest activity**, so guest usage data will not remain in the profile. **Allowing phone calls for guests** can also be turned off.

Within this profile, you can allow certain apps, streaming, and games, while still restricting phone calls or the installation of new applications, allowing you to create a much more controlled environment than if someone were just using your personal profile. Beyond profiles, the source of your applications is also important. With Mosaic OS, you are not required to download every app from the Google Play Store. Use the Aurora Store for this, which is easily available via the Mosaic Store. We have already demonstrated how to use it in a previous video. This is significant because apps installed via Google Play can operate in the isolated Google Play environment, and while they cannot see outside of this environment, they are able to access other apps located within that same space. This means that applications downloaded from Google Play are connected via Google Services, allowing them to communicate with each other and with Google as well, but they cannot see outside of their own sandbox environment. Conversely, apps installed via the Aurora Store can utilize the Mosaic OS isolation model. Individual applications operate in separate containers and by default do not see each other's data. You can control what the application can access.

Let's take a few popular apps as an example. Viber or Messenger do not require Google services to download. If you download these from the Aurora Store, you have the option to configure whether the app can access your photos, your contacts, or your files. If you only use it for messaging, you can even choose to disable the microphone entirely. Press and hold the icon of the selected application, then navigate to **App info** and **Permissions**. Disable any features you do not require. The same rule applies to network access as well.
Using the built-in network control in Mosaic OS, you can completely block the internet connection for any specific application. For instance, you could download the Google Camera app from Aurora for its image quality, and then revoke its network access, so the application cannot transmit data or send telemetry over the network. This is one of the important differences compared to many traditional mobile environments, where the ability to block internet access for individual applications might be more restricted.

We have already explained that Google services can operate within an isolated environment on Mosaic OS. Just imagine a sandbox, which is the playground for Google services. The applications that rely on Google Services to operate are placed within the sandbox, such as Gmail, YouTube, or Facebook. These apps can access resources within the sandbox, but they do not automatically gain access to the rest of your phone outside that isolated environment. On a standard Android smartphone, Google Services may be granted extensive access to your contacts, location information, the camera, or various other system functions, depending on your specific settings. In the Mosaic OS isolation model, however, these access rights can be defined much more strictly, so it is worth using applications that require Google in a separate profile. But if you still use only one account, you can still get better isolation compared to a traditional Android environment.

So if you want to use Gmail, first you need the Google Play Store, which can be installed from the Mosaic Store. By downloading this, you also gain access to the isolated Google Play environment, which creates a sandbox within your account. Regardless of that, it is still true that you can manage the permissions yourself within the **App Info** settings. Naturally, there are certain **Permissions** you can revoke, but doing so might cause the app to stop working properly. For example, with Gmail, if you cut off network access, it becomes unusable.

One of the keys to the security of Mosaic OS is isolation. With separate profiles, you can separate different parts of your life, and you decide what each application can access. Apps do not need to know everything about you.