USER ACCOUNTS FUNCTION

The first steps and initial settings were completed in the previous video. Now we will show you how to create multiple user accounts — and why having multiple user accounts is beneficial.

By using user accounts, you can achieve an even higher level of security and give applications even less chance to access your data. User accounts are not able to communicate with each other — essentially, it is as if they were separate devices.

To create user accounts, you need to adjust a few settings: Settings > System > Users. Create a new user. Once this is done, you will see that it feels like getting a brand-new phone — all settings must be configured from scratch, as we showed in a previous video. Notifications from every account will arrive in the main account (the first one), unless you switch back to the main account by selecting End Session from the locked home screen. This stops all applications and processes running in that account — effectively shutting down that account's operation. If you simply switch users without ending the session, notifications will continue to appear in the main account. You can further enhance security by setting up a Guest account, which can also be managed in the user settings.

From the home screen, swipe down twice to access the notification panel and reach the accounts section. The account icon will appear at the bottom of the screen. By tapping it, you can manage accounts, create new ones, and switch between them.

Once the accounts are ready, you can proceed with downloading applications. Compared to a traditional phone, there are additional steps here, because you can define precisely what permissions each application receives. By default, every application is locked inside a container. It cannot see anything on the phone. The application will request the permissions it needs for normal operation — and of course, these permissions must also be granted on this phone. However, applications often request access to features they have no legitimate need for.

On traditional phones, applications also communicate with each other and share data. This happens regularly in the background. On Mosaic OS, however, this is not possible.

1. Containerization

There are two ways to download applications. Some applications do not require Google Play Services to function. One alternative download option is F-Droid, which can be downloaded from fdroid.org. It is an app store containing only open-source applications. F-Droid guarantees that only applications that can be independently verified by anyone are listed on their platform. If many users have downloaded an app, it is likely to be reliable and verified.

From the F-Droid store, you can download Aurora Store. This allows you to install applications that you would otherwise download from the Google Play Store, but which can function without it. Due to Aurora's technical solution, downloads may not always succeed on the first attempt. You may need to try downloading an application multiple times. Once installed, you will find out whether the application is willing to operate without Google Play Services.

Applications downloaded this way are placed into a so-called CONTAINER. They cannot access anything on the phone except the functions explicitly permitted by the user. By default, Mosaic OS operates these applications in a way that prevents them from transmitting data outward.

2. Sandbox

If an application requires a Google user account, the Google Play Store does not function merely as an app marketplace — it effectively becomes a controller of the entire phone. Overriding our own settings, it allows applications to communicate with each other and continuously requests and forwards information from them.

On Mosaic OS, Google Play Services is confined within a Sandbox. In other words, it is given a playground where it can do what it wants — but it cannot see outside of it. It does not have access to the core foundations of the operating system or the deeper system-level capabilities of the phone. We can define what permissions the Sandbox receives, and the Google Play Store cannot override these settings.

We switch to the second user account so that applications downloaded from the Google Play Store will not have access to data stored in the first account. From the Mosaic Store, we download the Google Play Store, and from there we can obtain the additional applications we need. This is where the importance of user accounts becomes clear: in a separate account, we can completely isolate these applications. For example, if in the main account I make phone calls, use messaging services, and store family photos, then Google applications installed in the second account will not be able to access that data.

You can manage application permission requests in two ways. First, you can use quick tiles to disable microphone, camera, and location access. This setting applies to all applications on the phone — meaning that if you disable the microphone, you will not be able to make phone calls either.

It is better to use per-application settings. By long-pressing an app icon and tapping the “i” symbol, the App Info menu appears. Here, you can individually grant or deny each permission, ensuring that only the access truly required by the application remains active. You can even disable network access entirely.

By enabling Settings > Network & Internet > Data Saver, the system prevents certain applications from using mobile data in the background. Under the Unrestricted mobile data option, you can review and define which apps are still allowed to use mobile data in the background in this mode. By tapping the three dots in the top right corner and selecting Show system, you can also view system applications — it is advisable to disable those that are not necessary.

So, there are two main methods for downloading applications, as discussed earlier. If you follow these basic rules, your photos, chats, and phone conversations will be much safer. Use the Aurora Store and place Google applications in a separate account. And one more tip: it is also advisable to put your mobile banking app and any applications used for purchases into a separate account. This way, they too will be isolated from other applications.