

Hello everyone! We are continuing our presentation of settings that can make your Mosaic OS phone even more secure. These settings are entirely optional, so you can choose what feels comfortable and which daily changes you might be able to get used to over time. The main point is that with every single tiny adjustment you make, you are moving one step higher in terms of overall security. We cannot stress enough that Mosaic OS creates a safer environment for daily mobile use even with its default settings, than the most widely used operating systems. So let's look at the further settings!

1. **Settings → Security & privacy → Privacy controls → Permission manager:** please restrict app access in every single category. **Camera access** and **microphone access** are turned off globally. I have also placed it among my quick settings so that I can toggle it on or off with a single move, but even then, the microphone fails to work during calls.
2. **Settings → Security & privacy → Exploit protection → Auto reboot:** If the phone is inactive for the specified time, for example six hours, it will restart automatically. So if someone is currently attacking your phone and working on cracking the password, it could take them many hours or even several days, a restart could potentially prevent the process from completing successfully.
3. We go back one step, **Turn off Bluetooth automatically.** If you leave your Bluetooth turned on all the time, you are constantly broadcasting data that someone could potentially misuse. With this particular setting enabled, however, the device will not automatically connect to the hands-free system in your car. Pick a time, say one minute, so you won't have to manually turn off Bluetooth when you disconnect the headphones. It stops after one minute.
4. **Settings → Security & privacy → More security & privacy → Show media on lock screen** is currently turned off. **Allow Sensors permission to apps by default:** turned off. **Save screenshot timestamp to EXIF** is currently disabled. This is how you can send screenshots without any metadata attached. The phones we use today save extra information whenever you take a screenshot. It remembers, for example, the time, the time zone, and the device model. And if you forward the screenshot to someone, this information goes with it. With the Mosaic operating system, you can share a screenshot without including any additional information beyond the image itself.
5. We recommend that you add the option to block your location to the quick settings menu. By the way, this setting is also available within the **Settings** menu under the name **Location**. Turn off location, or if left on, manage **App location permissions below**. Here, you can block apps from accessing your location data. **Location services → Wi-Fi and Bluetooth scanning** are also turned off, meaning we do not allow applications to scan for Wi-Fi networks, even if, Wi-Fi is off. Furthermore, we do not permit applications to scan for nearby devices, even if Bluetooth is currently disabled.
6. We go back one step, **Secure User Plane Location**. This setting basically speeds up and makes the location determination more accurate. Set it to **GrapheneOS proxy** if you use map applications.
7. **Settings → System → Keyboard:** check every keyboard, restrict internet access and data collection, which you can do between the applications. Upon the very first time you power on your phone, you are given the option to download the Heliboard keyboard. By the way, you can also download this later from the Mosaic Store. It is a Hungarian-speaking open source keyboard that is completely customizable and secure.
8. **Settings → System → System updates:** The **Release channel** is basically **Stable**, meaning you only get the final versions of the updates. However, Mosaic OS is currently running in **Beta**. **Automatic reboot** is turned on, so after an update, if the device is inactive, it will automatically reboot.

Stay with us, because we will show many more features and options with which you can take back control over your data, and you can decide again, who and what can know about you.