Settings – 12+1 steps

We are continuing our presentation of the MosaicOS operating system. The emphasis continues to be on security and the protection of our data. This is also served by the Titan M two chip in Pixel phones, which provides hardware security and makes software attacks harder. However, by adjusting a few settings, we can further enhance the overall security. Basically, everyone has a different limit where they choose convenience at the expense of security, or in some cases the other way around, choosing security at the expense of convenience. These specific settings do not necessarily mean that if you skip even one of them or fail to use them exactly as written in the manual, your phone is no longer secure. However! MosaicOS offers much greater security with default settings than today's most popular operating systems. With these extra settings, we can further enhance the protection of our data. Everyone can decide for themselves which option is still comfortable to use. Therefore, we are presenting these now.

- You should try to avoid open networks whenever possible, and do not allow your phone to connect to them automatically. First of all, please navigate to the **Settings** menu, then **Network & internet**, and finally **Internet**. Then, scroll down until you reach the **Network preferences** section. Make sure that the **Turn on Wi-Fi automatically** is switched off. You never want your Wi-Fi to automatically turn itself on and broadcast signals anywhere at any time. Make sure that the **Notify for public networks** is switched off. We strongly advise against **Allow WEP networks**, and you should only ever use a WEP connection if it is the absolute only way you can get online. In all other cases, it should be avoided because such a network is vulnerable, and with the proper tools, the password can be cracked in a few minutes or hours.
Settings – **Security & privacy** – **Exploit protection** – **Turn off Wi-Fi automatically**: should be set to a timer. I choose one minute. This means that if I leave home and there is no Wi-Fi connection for one minute, the phone will automatically turn off the Wi-Fi. The shorter the time you choose, the better it is. If you choose to use your phone in this manner, you will have to manually configure whether you want to use Wi-Fi or mobile data at any given time.

- Now go to the **Settings** – **Network & internet** – **Hotspot & tethering** – **Wi-Fi hotspot** option. As often as possible, keep the **Wi-Fi hotspot usage** option turned off. If you still have to use it, the **Hotspot name** should not be something that identifies you or your phone, as this is also public. For the **Security** option, always choose the highest encryption supported by your device, and never choose the **None** option. **The WPA2 and WPA3 protocols** are responsible for the encryption of the password. Protocols below WPA2 are already very vulnerable, and they do not even appear here. However, not all devices support WPA3 yet. It is therefore the best option to select **WPA2/WPA3-Personal**, because this way the devices that support WPA3 will be able to utilize it, will connect with this, and those that do not, will connect with WPA2. Set a strong password for your hotspot. **Turn off hotspot automatically** should be checked, so if there is no connected device, the hotspot will stop by itself. If the **Data Saver** feature is currently enabled, you will not be able to use the hotspot.

- Now please navigate to the **Settings** menu, then **Network & Internet**, and finally **Private DNS**. Set that to **Automatic**. When you visit a website, your request passes through a DNS server. If you use a private DNS, not Google's for example, then the request does not go through Google's server, so Google will not see this activity. You can also use different

private DNS providers if someone wants to achieve even greater security, but for an average user, the **Automatic** option is perfectly fine. You should choose the **Private DNS provider hostname** option if you intend to use a private DNS provider. One of the most popular of these is Next DNS. Through its own website, Next DNS lists the instructions. By going through this process, you get an address that can be entered for the P**rivate DNS provider hostname**. This increases security by blocking advertising and malicious interfaces as well.

- Go to **Settings**, then **Network & internet**, and select **VPN**. This helps to make all of your online activities much more secure, it establishes a secure and fully encrypted tunnel between your internet connection and the VPN provider's server. An average user has no need for something like this.

- **Settings** – **Network & internet** – **Internet connectivity checks**: **GrapheneOS server** by default. You can leave this or turn it off. The point of this is whether the given network has an internet connection, and through what it is checked. The most important thing is that you should not use the **Standard (Google) server**.

- **Settings** – **Connected devices** – **See all**: this is where you can see every single one of your saved devices, tap the gear icon next to them to turn off unnecessary permissions.

- Go to **Settings**, then **Connected devices**, then **Connection preferences**, and finally **Bluetooth**: Ensure that your device name does not reveal your identity or your phone model. Never give your own name, as this is also public information.

- Go to **Settings**, then **Connected devices**, then **Connection preferences**, and turn on **NFC** temporarily, to access the next option. In order to use NFC, you are required to unlock your device first. Please check this box. Afterwards, go ahead and turn off **NFC**. We did this now because people usually keep NFC turned on, so NFC communication works even with a locked screen. This is really convenient because when you pay with your phone at the store, you just hold the phone up to the terminal and the payment is complete. But if someone has a pocket terminal or other device that can perform this same NFC communication, then anywhere, by simply holding the device close to your locked phone at any given moment, it was able to deduct the funds from it. It is not possible to make payments using Google Pay on MosaicOS, however, there are certain services that can still function in this manner.

- Go to **Settings**, then **Connected devices**, then **Connection preferences**, and **Printing**: ensure the **Default Print Service** is always disabled.

- Please navigate back to the main **Settings** page, then select **Apps**, **See all apps**, and carefully review the settings for each individual application, deny as many permissions as possible. This is a more time-consuming setting, as you can disable those accesses one by one for every application, which it does not need at all for its operation. For every single application, there is an option called **Background** data in the **Mobile data & Wi-fi options**. You should turn this off unless the app really needs to run in the background. This way, you also save battery life.

- Go to **Settings**, then **Apps**, and **Special app access**: check every single point one by one and restrict the applications. For instance, when it comes to **All file access**: do not allow applications to do that. **Install unknown apps**: Do not allow this setting, so if you wish to download anything, your phone will prompt you for confirmation once more. **Wi-Fi control**:

If this feature is turned on, the application is able to switch your Wi-Fi connection on or off. By tapping the three dots in the top right corner and selecting **Show system**, you can view system applications and apply restrictions to them too.

- **Settings**, **Notifications**, and **Enhanced notifications** are also off. The goal here is to stop receiving suggestions for various actions. Because expanded notifications, as the pop-up warning indicates, can gain access to your personal data, your contacts, and even your messages. So let us keep it switched off.

- **Settings** – **Display** – **Lock screen**: The primary goal here is to ensure that as little information as possible is displayed on the lock screen. **Notifications on lock screen** – **Compact view**: The best approach is to have all three of these options turned off. Perhaps the **Show viewed notification** icons option can be turned on. This means that the icon of the application sending the notification will be visible on the lock screen, but the content of the notification will not. If you switch over to the **Full list** view, you have the option here to **Show viewed notifications**. If you leave this checked, the content of the notifications will also appear on the locked screen. If, for example, you receive a message, you will not only see that you have received a message, but its full content as well, which is not a good option from a security perspective.

- We are taking one step back, **Add text on lock screen**: None. **Use device controls** are currently disabled. This could also be an attack surface. If you connect an external device to the phone that effectively has admin rights, then it will be able to control the phone. If you turn this option off, then with a locked phone this option does not work. **Tap to check phone** turned off. **Lift to check phone** turned off. Wake screen for notifications turned off. This way the locked screen does not signal upon any notification, you can only see the notification after unlocking. We step back one. **Screen timeout**: The shorter it is, the better. One or two minutes is ideal. After that, the phone will lock itself automatically.

By adjusting these settings, you are taking significant steps toward ensuring that the data and information on your phone remain as secure as possible. This does not imply that if you do not follow even a single one, using MosaicOS is entirely useless. We developed this operating system so that even when used with the default settings, it creates much more secure conditions for your information, than the most common operating systems used today.