# Get full access to your smartphone

Firmware is the permanent software that a manufacturer programmes into a device?s read-only memory. They run in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc. Most functionalities are 'locked in' so the user is not capable of controlling or altering these functions. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to alter the programs running the smartphone. The process of overcoming these manufacturer imposed limits on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Successful rooting or jailbreaking will enable you to install additional applications, make modifications, and give you total control over data storage and memory of the smartphone in order to make it more secure.

*WARNING:* Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

* There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
* The manufacturer or mobile carrier warranty may be voided.
* In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

Rooting or jailbreaking is a complex process and different for every device. Search the internet for instructions on the best way to root your own device.

# Alternative Firmware

Rooting your phone will allow you to install alternative firmware.  
An example of an alternative firmware for some Android phones is [Cyanogenmod](http://cyanogenmod.com/) which allows you to uninstall applications from the system level of your phone. By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge. This sort of alternative firmware includes features such as the automatic concealment of your location when online by using a Virtual Private Network as default, and automatic incognito browsing meaning history of your communication is not recorded on your smartphone.

# Encryption of volumes

Rooting your phone will also allow you to encrypt its entire data storage or create a volume on the smartphone to protect certain information.

Luks Manager allows easy, on-the-fly strong encryption of volumes with a user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the [Luks Manager](https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=en) provides to store all your data.

# Data encryption tools

The Android Privacy Guard (APG) allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.  
You can learn how to install and use it in the [APG Guide](umbrella://lesson/k9-&-apg) in the tool kit.

[Cryptonite](https://code.google.com/p/cryptonite/) is another open source files encryption tool with more advanced features on it, and specially prepared for rooted Android phones with a custom firmware.

Swipe right for this lesson's checklist

Go to the Beginner lesson for advice on the dangers of using mobile phones.

[Go to Beginner Lesson](umbrella://lesson/mobile-phones/0)

### RELATED LESSONS/TOOLS

* [APG Guide Tool](umbrella://lesson/k9-&-apg)

### FURTHER READING

* [Security in a Box ? Chapter 11, Use smart phones as securely as possible](https://securityinabox.org/en/guide/smartphones)