Smartphone and tablets (all types)

SECURE YOUR MOBILE DEVICE

Everyone can benefit from having a secured smartphone that protects their personal data. However, mobile security is particularly important for organisations that work in fragile contexts where access to sensitive data can be highly contentious (human rights, health, protection, war zones…)

2017

WHAT IS THE PURPOSE ?

Securing your smartphone ensures that the personal data stored on the phone is protected and is only accessible and visible to authorised persons.

Prerequisites

- None

When working with sensitive data, security needs to be guaranteed at three different levels: (1) password-protected access to the mobile device, (2) data storage using encryption and (3) transmission with an application that encrypts the data and uses a secure connection (HTTPS). If just one of these levels fails, the security of the mobile device will be compromised.

RECOMMENDED GENERAL PRACTICES:

- ***Lock the screen***
  - In the security settings, choose to lock the screen with a PIN code or password (according to your own preference).
- ***Active the automatic screen-lock***
  - In the security settings, choose to automatically lock the screen if the device is inactive for more than a minute.
- ***Choose a strong password or PIN code to reduce the risk that it can be hacked):***
  - For PIN codes, do not use a year or date of birth and use a unique code for each device.
  - For passwords, do not choose an existing word. Mix numbers and letters to create a password with more than 8 characters and never leave a note of the password in an unsecured place.
  - Suggestion: create a password from an easy to remember phrase by remembering the first letters of each word in the phrase.

FOCUS ON SENSITIVE DATA:

- ***Limit unnecessary connectivity***
  - Disable features that you do not use, such as Bluetooth, Wi-Fi et GPS.
  - Turn off the device when it is not in use.
- ***Activate device encryption***
  - In the security settings, click to encrypt the device.
  - Encryption may take longer than an hour.
  - Even when the device is encrypted it will still be possible to use and read the data in your applications.
- ***Clear information that is no longer useful***
  - Clear all sensitive information when you no longer need it.
- ***Send data securely***
  - Never use SMS, a 3G connection or Bluetooth.
  - Never use a public Wi-Fi connection (or a connection without a password).
  - Use applications that use end-to-end encryption such as WhatsApp or Telegram (not Skype).
  - For applications that use the internet, make sure that they use an HTTPS protocol (not HTTP).

Data security is an extremely complex subject. Where necessary, we strongly recommend that you contact an expert for advice. You can find out more about this subject in this digital security guide for activists and human rights defenders and this report on the use of mobile messaging applications in the humanitarian sector.

Free

1-2 hours