CCN-CERT

BP/03

Mobile devices

BEST PRACTICES REPORT

MAY **2021**

Edit:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.06.09 17:44:20 +02'00'

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set forth herein, expressly disclaiming any implied warranties of any kind that may be found to be related. In no event shall the National Cryptologic Centre be held responsible for direct, indirect, incidental or extraordinary damage derived from the use of the information and software indicated, even if advised of the possibility of such damages.

LEGAL NOTICE

The partial or total reproduction of this document by any means or procedure, including reprographics and computer processing, and the distribution of copies thereof by public rental or loan, are strictly prohibited without the written authorization of the National Cryptologic Center, under the sanctions established by law.

Index

1. **About CCN-CERT** 4
2. **Introduction** 5
3. **Good practices in the configuration and use of mobile devices** 8
    - 3.1 Lock screen 9
        - 3.1.1 Access code or digital fingerprint 9
        - 3.1.2 Functionality from lock screen 12

    - 3.2 Communications via USB 14
    - 3.3 Updating the operating system and applications 17
    - 3.4 Encryption of the mobile device 18
    - 3.5 Default configuration 20
    - 3.6 Back-up copies 21
    - 3.7 Remote management of the mobile device 22
    - 3.8 Wireless communication capabilities 24
        - 3.8.1 NFC (*Near Field Communications*) 25
        - 3.8.2 Bluetooth and Bluetooth Low Energy (BLE) 25
        - 3.8.3 Wi-Fi 26
        - 3.8.4 Telephony networks: messaging/voice and mobile data (2/3/4G) 27
        - 3.8.5 Localisation capabilities and services 28

    - 3.9 Mobile applications (apps) 29
        - 3.9.1 Installing apps 29
        - 3.9.2 App permissions 31
        - 3.9.3 E-mail 32
        - 3.9.4 Messaging applications 32
        - 3.9.5 Social medias 35
        - 3.9.6 Web browsing 36

4. **Other generic recommendations** 40
5. **Decalogue of recommendations** 42

1. About CCN-CERT

The **CCN-CERT** is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, assigned to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity**, by being the national alert and response center that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centers.

Its ultimate aim is to make **cyberspace more secure and reliable**, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

> **The CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN.**

2. Introduction

> **The proliferation of mobile devices makes it necessary to examine the security provided by this type of device with regard to the information they manage, both within corporate environments and in the private sphere.**

In recent years, the development of mobile devices and communications along with wireless technologies has revolutionized the way we work and communicate. The increasing use of these technologies makes mobile devices a prime target for attackers.

The proliferation of mobile devices, together with the development of their capabilities, features and possibilities of use, makes it necessary to examine the security provided by this type of device with regard to the information they manage, both within corporate environments and in the private sphere.

A mobile device is an electronic device for personal or professional use that is small in size and allows the management (storage, exchange and processing) of information and access to communications networks and remote services, both voice and data, and usually has telephony capabilities, such as mobile phones, smartphones (advanced or intelligent mobile phones), tablets and PDAs (*Personal Digital Assistant*) regardless of whether they have a physical keyboard or a touch screen.

2. Introduction

The level of awareness of real threats is not sufficiently high among end-users and organizations, despite the fact that mobile devices are used for personal and professional, private and relevant communications, and for the storage and exchange of sensitive information. Not only organizations are often the target of numerous attacks, but also users' non-corporate information (personal data).

Lately, a notable increase has been identified not only in the number of specimens of malicious code for mobile devices (mobile malware), but also in their complexity and sophistication, with Spain being among the most affected countries worldwide based on the number of infections.

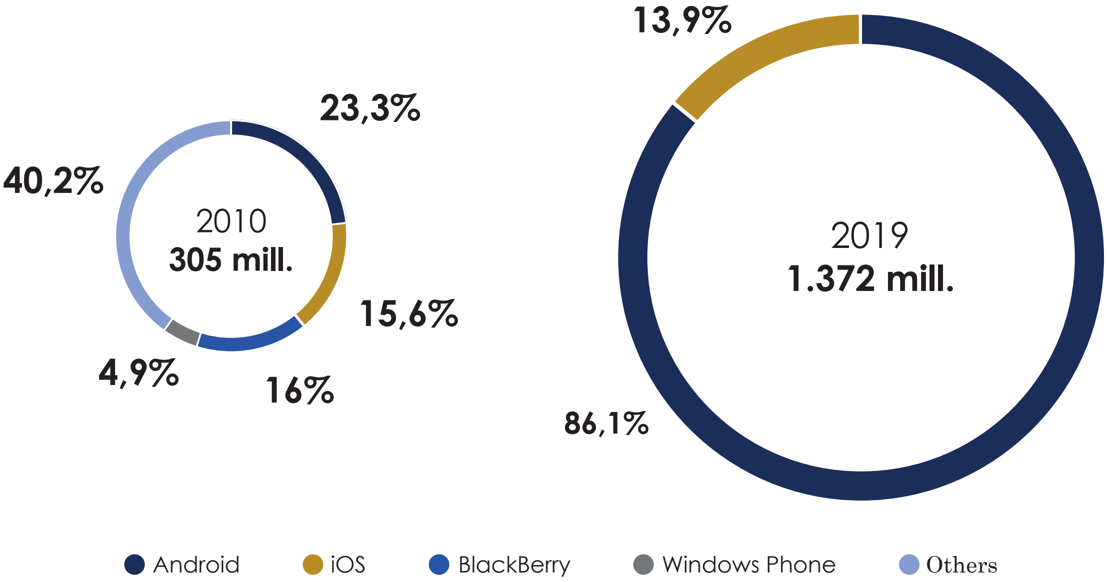


Figure 2-1 Global market share of mobile devices. Source: IDC[1]

Awareness, common sense and good practices in the configuration and use of mobile devices are the best defense to prevent and detect such incidents and threats .

---

[1] "Worldwide Smartphone OS Market Share". IDC. Report. Q2 2015. http://www.idc.com/prodserv/smartphone-os-market-share.jsp

2. Introduction

Because there is widespread industry adoption, both at the enterprise and personal level, of two of the mobile platforms above all others, Android (Google) and iOS (Apple), most of the examples used in this guide refer to these two mobile platforms[2].

The purpose of this document is to describe these practices **in order to help end users protect** and make the safest possible use of their mobile devices, by going into more detail on the configuration and use of protection mechanisms.

To this end, a **set of security guidelines and recommendations** will be offered to mitigate possible harmful actions, providing information on the most common attack techniques, as well as the resources used by attackers to infect mobile devices or obtain personal information from a victim.

---

[2] It should be noted that there are significant differences in the configuration and use of mobile devices depending on the particular version of Android or iOS available.

3. Good practices in the configuration and use of mobile devices

The set of recommendations shown below is divided into multiple groups, each related to the different capabilities and functionalities offered by mobile devices, such as: **improving protection against unauthorized physical access to the device**, r**educing the impact of loss or theft of the device**, or **improving the confidentiality and security of information storage** and of **communications with other remote services and systems**.

The aim of these recommendations is to enable users to increase the level of protection and security of their mobile devices, both from the point of view of their configuration and their daily use, thus avoiding falling victim to any of the aforementioned attacks.

It should be borne in mind that some of the features described above, and therefore the security recommendations put forward, are dependent on the type of operating system used by the mobile device (Android, iOS, Windows Phone, etc.), the version of the device, the manufacturer and the specific model associated with it.

Therefore, not all of the recommendations provided will necessarily apply to all existing mobile devices. In any case, it is recommended to implement as many recommendations as possible.

> **The aim of these recommendations is to enable users to increase the level of protection and security of their mobile devices, thus avoiding falling victim to any of the aforementioned attacks.**

3.1 Lock screen

The lock screen is the primary defense mechanism against unauthorized physical access to the phone by potential attackers.

Modern mobile devices are very attractive for theft or robbery due to both their economic value (of the *hardware* itself) and the value associated with the sensitive and personal information they store.

For this reason, the screen should be protected by an access code and remain locked for as long as possible. It is also recommended to limit the functionality available on the lock screen to third parties who do not know the access code.

3.1.1 Access code or digital fingerprint

In order to be able to access the mobile device and to have access to all the functionality offered by the mobile device, **it is recommended to protect the mobile device by means of an access code associated with the lock screen**.

Although this code will be requested from the user on multiple occasions throughout the day, **it is necessary to select a robust access code**, of at least six (6) or eight (8) digits, and preferably combining letters and numbers. Under no circumstances is it recommended to use a four (4) digit PIN or access code, which is, however, commonly and widely used.

Additionally, in order to keep exposure of the mobile device to unauthorized access, even temporary, to a minimum, **it is recommended that the device be configured to request the access code immediately after the screen is turned off, which should automatically lock as soon as possible if there is no user activity** (e.g. after one minute).

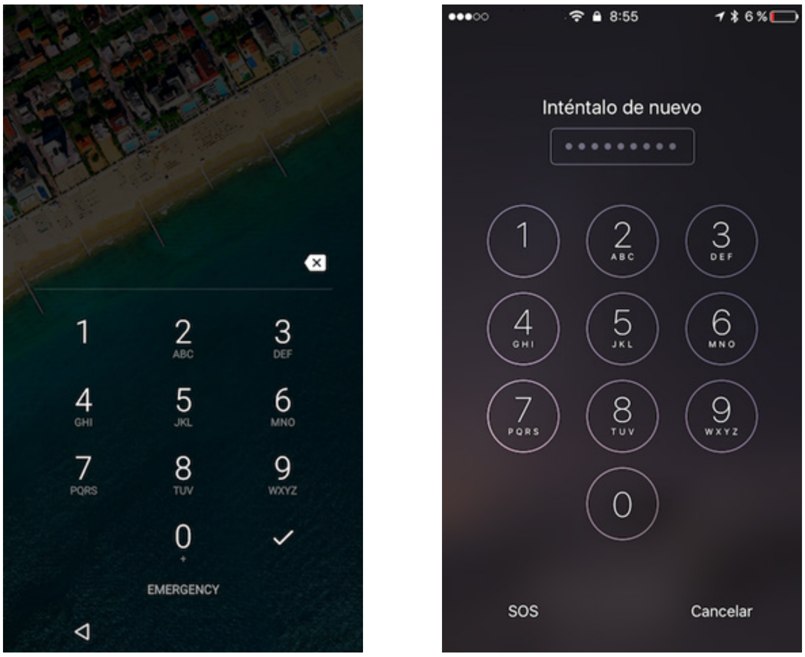
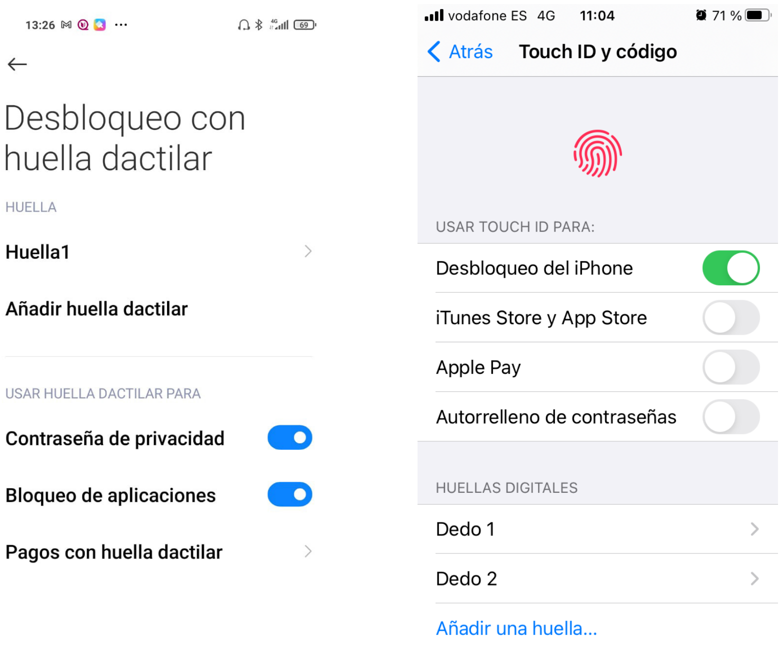


Figure 3-1 Passcode lock screen on Android and iOS.

In order to find the right balance between security and functionality, as the user has to unlock the phone dozens of times a day to make use of it, it is recommended to configure the fingerprint unlock functionality (in those devices that have this capability and fingerprint sensor) complemented by a strong passcode.

This functionality provides the mobile device with a protection mechanism and makes its use as comfortable as possible for the user.



13:26

Desbloqueo con huella dactilar

HUELLA

Huella1

Añadir huella dactilar

USAR HUELLA DACTILAR PARA

Contraseña de privacidad: on

Bloqueo de aplicaciones: on

Pagos con huella dactilar

vodafone ES 4G 11:04 71 %

Atrás — Touch ID y código

USAR TOUCH ID PARA:

Desbloqueo del iPhone: on

iTunes Store y App Store: off

Apple Pay: off

Autorrelleno de contraseñas: off

HUELLAS DIGITALES

Dedo 1

Dedo 2

Añadir una huella...

Figure 3-2 Fingerprint lock screen on Android and iOS.

3.1.2 Functionality from lock screen

Users can access several functionalities quickly and easily from lock screen without unlocking the device, such as receiving and answering messages or phone calls, receiving notifications of events and reminders, accessing the camera, modifying some settings such as wireless communication capabilities (Bluetooth, Wi-Fi, 2/3/4G, etc.) and managing the airplane mode, accessing information from specific applications (apps), such as weather or investment information, or interacting with personal digital assistants, such as Siri on iOS, Google Assistant (or Google Now) on Android or Cortana on Windows (Phone).

The possibility for third parties to use these functions without knowing the access code has very relevant implications from a security point of view.

For example, a potential attacker who gains unauthorized access to the mobile device (after it has been lost or stolen), could activate the device's airplane mode, disrupting all communications of the mobile device with other remote networks and services, and disabling therefore, the remote management feature that allows the user to detect the current location of the device, or to remotely delete the data stored on it (see section "3.7. Remote management of the mobile device").

Additionally, multiple vulnerabilities have been identified over time based on the use of these features, which allow bypassing the lock screen and passcode of the mobile device[3].

---

[3] "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Blog Post. October 2016. http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

It is therefore recommended to limit and minimize as much as possible the functionality available from the lock screen when the passcode is not entered. To this end, it is recommended to disable Google Assistant (or Now) and remove the most critical icons from the Quick Settings access control panel available at the top of Android (functionality available on Android 7.0 or higher versions), while for iOS it is recommended to disable Siri, the Control Centre available at the bottom or the Notification Centre, as well as any other relevant functionality.

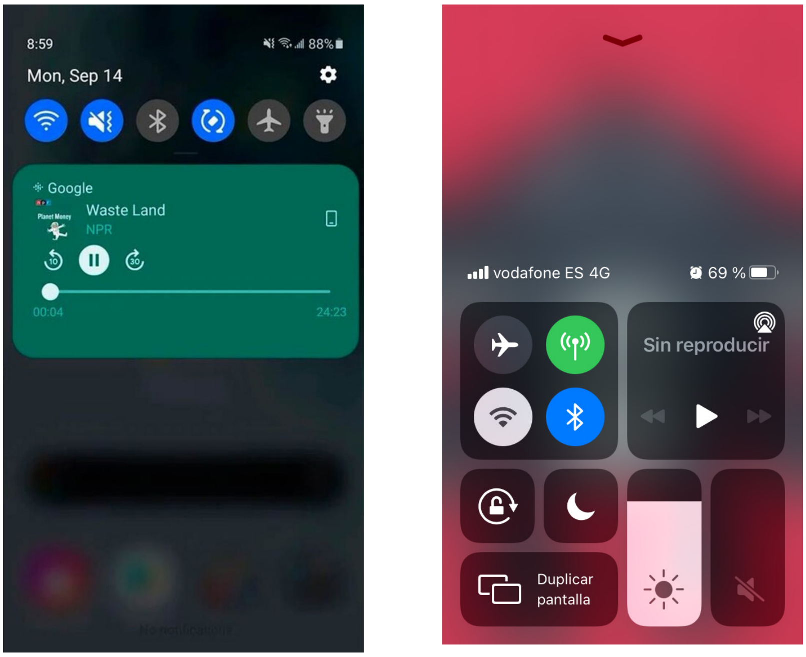


Figure 3-3 Sensitive functionality available from the lock screen on Android and iOS.

3.2 Communications via USB

The charging and synchronization ports of mobile devices, normally located on the bottom of the device, allow wired connection via USB port to a computer or plug. The USB connection provides two (2) functionalities: on the one hand, it allows to charge the battery of the mobile device, and on the other hand, it allows data exchange.

Juice jacking is an attack that consists of stealing data from users or installing harmful apps on their devices when they connect them to fake charging stations.

Due to the fact that one of the current limitations of mobile devices is battery capacity and life, with users sometimes having to charge their mobile devices in the middle of the day and with some urgency, attackers have used this dual functionality of USB connections or communications to compromise devices through data connection, posing as charging stations in public places, an attack known as *juice jacking*.

Through this attack, it is potentially possible to extract personal data stored on the mobile device, as well as to carry out more harmful actions, such as installing malicious *apps*:

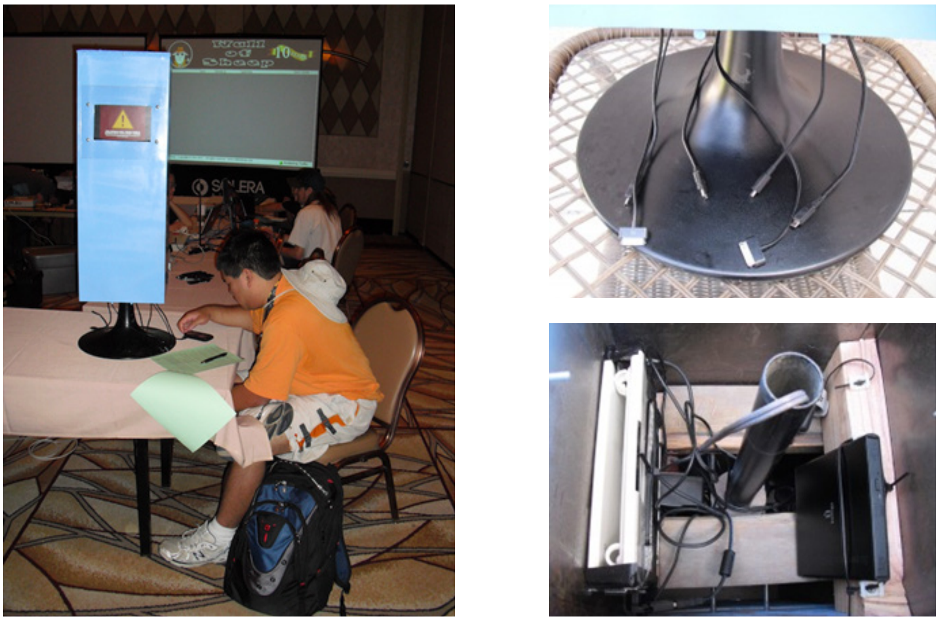


Figure 3-4 Juice jacking attacks. Source: KrebsonSecurity[4]

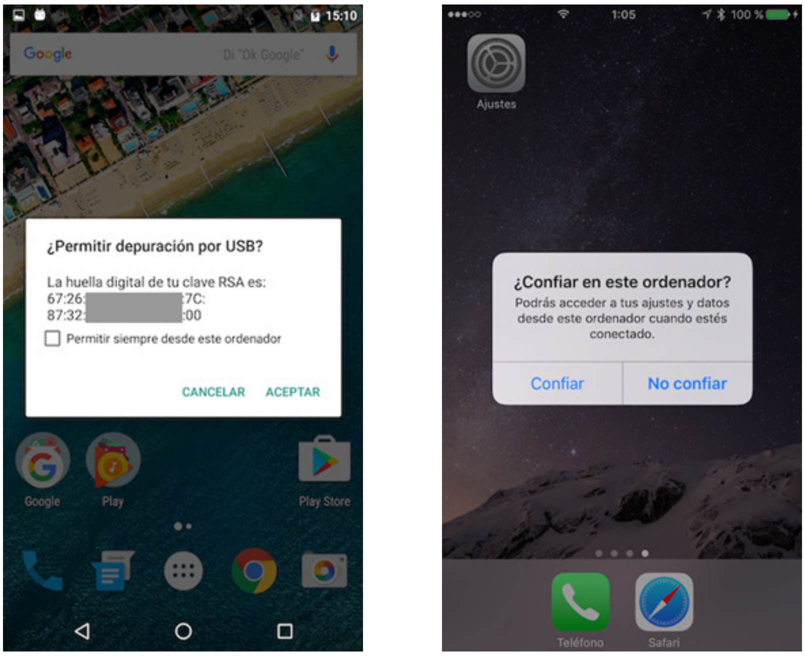
---

[4] "Beware of Juice-Jacking". KrebsonSecurity. Blog Post. August 2011. https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Modern operating systems have implemented safeguards against such attacks, so the first time the mobile device is connected to a computer via USB a trust relationship must be established.

The mobile device will ask the user if they wish to establish such a trust relationship, and it must be unlocked beforehand to confirm the request.

It is therefore recommended not to connect the mobile device to unknown USB ports and not to accept any trusted relationship via USB if you do not know if you are connecting the mobile device to a trusted computer.



¿Permitir depuración por USB?

La huella digital de tu clave RSA es:
67:26:[redacted]:7C:
87:32: :00

☐ Permitir siempre desde este ordenador

¿Confiar en este ordenador?

Podrás acceder a tus ajustes y datos desde este ordenador cuando estés conectado.

Figure 3-5 Establishing trust relationships via USB on Android and iOS.

3. Good practices in the configuration and use of mobile devices

USB capabilities of mobile devices also allow the installation of apps (see section 3.9). In order for a potential attacker to succeed in installing an app, the mobile device must have an insecure configuration that facilitates this type of communication (in the case of Android) and/or the phone must be unlocked (in the case of Android and iOS).

To prevent the installation of apps via USB, **it is recommended (depending on the mobile platform) not to enable the USB debugging capabilities of the mobile device**, available specifically for *app* developers, **and not to leave the mobile device unattended while unlocked**.

3.3 Updating the operating system and applications

Mobile devices have a mobile operating system (Android, iOS, Windows Phone, etc.), also called *firmware*, which provides all existing functionality by default, and which also includes a set of mobile applications that have been installed by default by the manufacturer of the operating system, the device or the telecommunications operator.

In addition, the user can install other third-party *apps* from the official application markets or from other repositories (see section 3.9 "Mobile applications (apps)").

It is recommended to always have an up-to-date operating system on the mobile device. It is also recommended to **always have the latest update for all apps installed on the mobile device.**

The latest version of both the operating system and apps addresses publicly known vulnerabilities and thus significantly reduces the device's exposure to attacks.

There are offensive tools that exploit vulnerabilities in mobile devices and can compromise the device by simply opening a text message (SMS) or multimedia message (MMS), or visiting a web link (without the need to download or execute any files) by exploiting weaknesses in the web browser or operating system.

Since offensive tools sometimes have *0-days* (*exploits* for unknown vulnerabilities that have not been patched), it **is advisable for the user to be very cautious about opening unsolicited, unknown or strange messages or web links**.

> **The latest version of both the operating system and apps addresses publicly known vulnerabilities and thus significantly reduces the device's exposure to attacks.**

3.4 Encryption of the mobile device

A critical feature in protecting the data and information stored locally by the mobile device is the encryption of its internal memory, used as the primary storage unit, as well as any other external storage unit, such as an SD (*Secure Digital*) card.

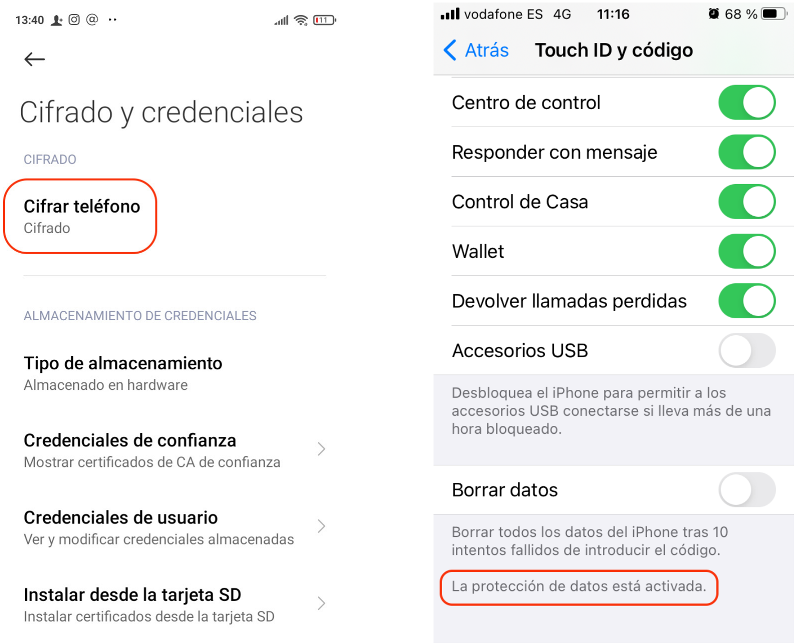
Capabilities to encrypt the memory of the mobile device are essential against unauthorized physical access to the mobile device by a third party, as it would otherwise be possible to extract the contents of the mobile device's memory chip and gain access to all stored information.

Regardless of the fact that some apps encrypt their data before storing it, it is recommended to make use of the native encryption capabilities of the mobile device, in order to protect all data and information associated with the user or organization stored on the mobile device.

In order to make use of these capabilities, it is essential to establish an access code for the mobile device, which should be robust (see section 3.1.1 "Access code or fingerprint"), as it will be used during the encryption process.

It is recommended to make use of the native encryption capabilities of the mobile device, in order to protect all data and information associated with the user or organization stored on the mobile device.

Some mobile devices such as iOS automatically activate encryption capabilities once a passcode is set, a scenario indicated by the text *"Data protection is enabled"* while others such as Android require the encryption mechanisms to be activated intentionally.



13:40

Cifrado y credenciales

CIFRADO

Cifrar teléfono
Cifrado

ALMACENAMIENTO DE CREDENCIALES

Tipo de almacenamiento
Almacenado en hardware

Credenciales de confianza
Mostrar certificados de CA de confianza

Credenciales de usuario
Ver y modificar credenciales almacenadas

Instalar desde la tarjeta SD
Instalar certificados desde la tarjeta SD

vodafone ES 4G 11:16 68 %

Atrás **Touch ID y código**

Centro de control ●
Responder con mensaje ●
Control de Casa ●
Wallet ●
Devolver llamadas perdidas ●
Accesorios USB ○

Desbloquea el iPhone para permitir a los accesorios USB conectarse si lleva más de una hora bloqueado.

Borrar datos ○

Borrar todos los datos del iPhone tras 10 intentos fallidos de introducir el código.

La protección de datos está activada.

Figure 3-6 Enabling native encryption capabilities on Android and iOS. Source: EFF[5]

In case the mobile device has a slot for an external storage drive, typically based on the use of SD memory cards, **it is recommended to make use of encryption capabilities to protect the contents of the external storage drive**.

In many cases it is not possible to encrypt such content, so it is recommended not to store any sensitive data or information on the SD card, such as corporate documents.

---

5. https://ssd.eff.org/en/module/how-encrypt-your-iphone

3.5 Default configuration

Mobile devices, after their initial activation, have a default configuration that, on the one hand, can be insecure and enable functionalities that could be used by a potential attacker to compromise them and, on the other hand, contribute to revealing unnecessary information about the device itself and/or its owner.

For example, it is common that when the mobile device is activated, most of its services and capabilities remain active, so that the user can make immediate use of them, such as the Bluetooth or Wi-Fi wireless interface, the personal digital assistant or cloud synchronization services.

On newer mobile devices, other services, considered more critical from a user's privacy point of view, such as location services, must be manually activated by the user during the initial configuration process of the mobile device.

It is recommended to disable all services and functionalities of the mobile device that are not going to be used permanently by the user.

Instead, it is recommended to enable them only when they are going to be used and to disable them inmediately after use.

In addition, information about the device itself and/or its owner, such as the device manufacturer and model or the owner's name, can be disclosed through the name of the mobile device, which is broadcast over data communications networks or through other wireless communications, such as Bluetooth, or when setting up a Wi-Fi hotspot to share the 2/3/4G mobile data connection.

It is recommended to modify the existing default configuration of the mobile device, removing any reference to the technical characteristics of the device itself and/or its owner.

3.6 Back-up copies

Protection of the information and data stored and managed by the mobile device should extend to scenarios of loss or theft of the mobile device, as well as hardware damage that prevents access to the contents on its main storage unit (or external drives).

To prevent data loss, **the user should make regular and preferably automatic *backups* of all contents of the mobile device to be protected and preserved**, preferably locally via USB or wireless Wi-Fi communication with the user's computer.

Alternatively, use can be made of the cloud backup capabilities associated with major mobile platforms, via wireless communication.

However, the user should be aware that the ease and convenience associated with these remote backup mechanisms has implications for the privacy and security of their data, as it will be transferred to and stored on a server managed by a third party (in the cloud).

3.7 Remote management of the mobile device

Modern mobile devices and remote management capabilities provided by device manufacturers through their mobile platforms and cloud services, such as iCloud[6] in the case of iOS or Device Manager [7] in the case of Android, allow users to potentially know the current location of their mobile device, to lock it when unlocked, to make it ring to identify its nearby location, to display a message so that whoever finds it can contact the owner, or to remotely erase the data stored on it.

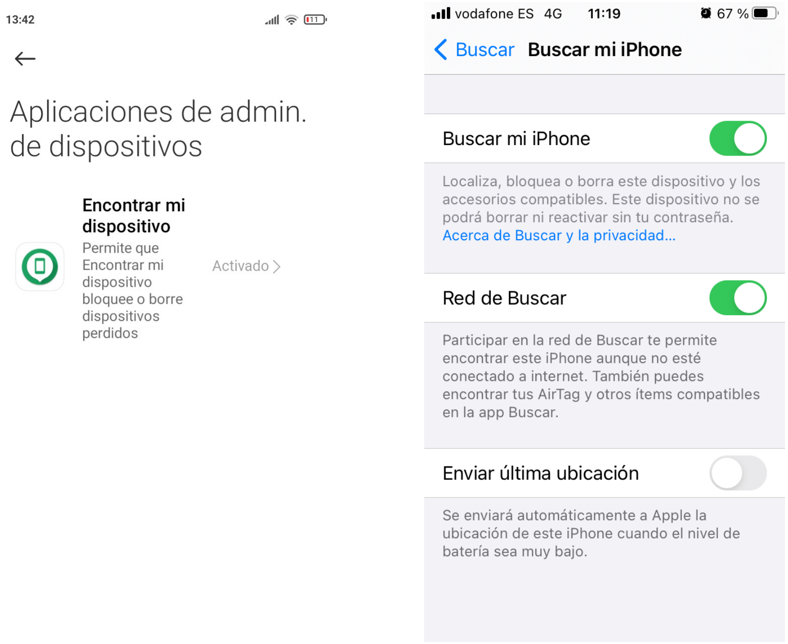
The user is recommended to familiarize himself with the remote management capabilities of the mobile device and its associated mobile platform, and to check the correct functioning of this service and all its functionality before it is necessary to make use of it in a real scenario following the loss or theft of the mobile device.

In order to make use of these services, the user must have an account on the manufacturer's platform, such as an Apple ID (user ID) for iCloud (iOS) or a Google user account for Device Manager (Android). The mobile device must also be associated with the user's account on the manufacturer's platform.

---

6. iCloud. Apple. Web. https://www.icloud.com
7. Android Device Manager. Google. Web. https://www.google.com/android/devicemanager

In addition, the “Find My iPhone” (or iPad on iOS) and “Device Manager” (on Android) functionality must be enabled and correctly configured on the mobile device:



13:42

Aplicaciones de admin. de dispositivos

Encontrar mi dispositivo
Permite que Encontrar mi dispositivo bloquee o borre dispositivos perdidos
Activado

vodafone ES 4G 11:19 67 %

Buscar **Buscar mi iPhone**

Buscar mi iPhone ●

Localiza, bloquea o borra este dispositivo y los accesorios compatibles. Este dispositivo no se podrá borrar ni reactivar sin tu contraseña. Acerca de Buscar y la privacidad...

Red de Buscar ●

Participar en la red de Buscar te permite encontrar este iPhone aunque no esté conectado a internet. También puedes encontrar tus AirTag y otros ítems compatibles en la app Buscar.

Enviar última ubicación ○

Se enviará automáticamente a Apple la ubicación de este iPhone cuando el nivel de batería sea muy bajo.

Figure 3-7 Enabling remote management capabilities on Android and iOS

It should be noted that many of these remote capabilities will not be truly operational if the management platform cannot contact the mobile device (or vice versa) or if the device is not able to obtain its location.

There are many reasons and scenarios in which communication between the management platform and the mobile device cannot be established, or the current location cannot be obtained, such as the mobile device being switched off, the battery running out, no coverage of the 2/3/4G mobile data networks or no known Wi-Fi network nearby, airplane mode activated, being in the basement or garage of a building, etc.

3.8 Wireless communication capabilities

Other important security aspects related to the confidentiality and integrity of data exchanged over communication networks are described below.

Many of the existing functionalities of mobile devices involve the use of data communications with remote platforms, in which various technologies and services are involved. Understanding usage scenarios and the functioning, at least in a generic way, of these technologies will allow a deeper understanding, firstly, of the security gaps they present and, secondly, of why it is necessary to take some protection measures to fill and improve these gaps.

Generally, **it is recommended to disable all wireless communication interfaces on the mobile device that will not be permanently used by the user**. Instead, it is recommended to enable them only when they are going to be used and to disable them again when unused.

3.8.1 NFC (*Near Field Communications*)

NFC capabilities in mobile devices enable short-range wireless communications and are currently used for access control and mobile payments, as they are integrated with *apps* and bank cards.

Having the NFC interface active at all times could allow a potential attacker, sufficiently close to the mobile device, to force fraudulent transactions and payments[8].

Having the NFC interface active at all times could allow a potential attacker, sufficiently close to the mobile device, to force fraudulent transactions and payments.

3.8.2 Bluetooth and Bluetooth Low Energy (BLE)

Bluetooth and BLE technologies are widely used today for the integration, monitoring and control of multiple electronic devices, such as personal devices or *wearables* (such as *smartwatches*), vehicles (hands-free) or devices associated with the *Internet of Things* (IoT). The mobile device itself acts as the brain or central controller of the digital world around it.

As a consequence, having the Bluetooth interface active at all times could allow a potential attacker to manipulate the communications and actions associated with the other devices or the information exchanged between them[9].

---

8. "New Android NFC Attack Could Steal Money From Credit Cards Anytime Your Phone Is Near". Blog Post. May 2015. https://www.player.one/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497#:~:text=Gadgets-,New%20Android%20NFC%20Attack%20Could%20Steal%20Money%20From,Anytime%20Your%20Phone%20Is%20Near&text=This%20attack%2C%20delivered%20through%20poisoned,are%20near%20the%20victims'%20phone

9. "Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable". Blog Post. August 2016. https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

3.8.3 Wi-Fi

The Wi-Fi interface is probably the most widely used communication mechanism in mobile devices today for exchanging data and accessing remote services and applications.

Having the Wi-Fi interface active at all times can allow a potential attacker to impersonate any of the different Wi-Fi networks known to the mobile device and to which it usually connects (such as the Wi-Fi network of the office, home, library, cafeteria, etc.), forcing its automatic connection to capture all the traffic generated/received by the mobile device and launch attacks directly against it[10].

Additionally, **it is recommended not to connect the mobile device to open public Wi-Fi networks (or Wi-Fi *hotspots*) that do not implement any kind of security**. Even if there is no cost associated with their use, the user's personal information would be at risk. Using such networks allows a potential attacker to intercept and manipulate all traffic exchanged by the mobile devic[11].

Instead, use Wi-Fi networks that are trusted and have security mechanisms (such as WPA2-PSK) configured. In the rare case where you need to use a public Wi-Fi network, a VPN (*Virtual Private Network*) service should be used to encrypt all traffic transmitted over the Wi-Fi network.

---

[10] "Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". DinoSec. Blog Post. February 2015. http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html

[11] "Avast free Wi-Fi experiment fools Mobile World Congress attendees". Avast. Blog Post. February 2016. https://blog.avast.com/2016/02/24/avast-free-wi-fi-experiment-fools-mobile-world-congress-attendees/

3.8.4 Telephony networks: messaging/voice and mobile data (2/3/4G)

One fundamental capability offered by most modern mobile devices is the possibility to connect to mobile phone networks for voice, messaging and data services (2/3/4G).

It is assumed that these capabilities will be active on mobile devices most of the time, in order to be able to make and receive calls, messages and communicate with remote services and applications when a trusted Wi-Fi network is not available nearby. It is therefore necessary to be aware of the weaknesses of these technologies that started to spread in the late 1980s[12] in Europe (GSM).

2G telephony networks, which still exist today, do not make use of security mechanisms that allow the mobile device to be sure that it is connecting to the legitimate network of the telecommunication operator (known as mutual authentication).

Consequently, an attacker could spoof the legitimate network (similar to what happens with Wi-Fi networks), forcing the device's automatic connection and intercepting communications with devices known as IMSI-Catchers or Stingrays[13].

It is recommended that under no circumstances should the user give priority to 2G networks on their mobile device over 3G or 4G networks, even though battery consumption is higher on the latter due to, among other things, their higher data transfer capacities. If possible, the use of 2G networks should be disabled.

---

[12] http://www.gsmhistory.com/who_created-gsm/

[13] "Surprise! Scans Suggest Hackers Put IMSI-Catchers All Over Defcon". Blog Post. August 2016. http://motherboard.vice.com/read/surprise-scans-suggest-hackers-put-imsi-catchers-all-over-defcon

3.8.5 Localization capabilities and services

Finally, location capabilities and services in modern mobile devices, which allow to locate the phone around the globe via the GPS satellite system or through Wi-Fi networks and mobile phone towers, has opened up a wide range of services and possibilities.

However, obtaining and sharing the location of the mobile device constantly, even in real time, and therefore of its owner, has very relevant implications from the point of view of users' privacy and security.

On the one hand, services that make use of these capabilities can monitor where the user is at all times. On the other hand, users can, on purpose or inadvertently, broadcast their current or past location through the metadata of photographs taken with the mobile device and subsequently published, through messages on social networks or through the use of other *apps*[14].

It is recommended that the user disables location services if they are not being used, and if they are being used, to restrict as much as possible both the intentional use of these services and access to these services by the *apps* installed on the mobile device, desactivando el disabling the associated permission for most *apps*.

---

[14] "How mobile apps leak user data that's supposedly off-limits". Sophos. Blog Post. February 2016. https://nakedsecurity.sophos.com/2016/02/29/how-mobile-apps-leak-user-data-thats-supposedly-off-limits/

3.9 Mobile applications (*apps*)

Mobile devices such as *smartphones* are considered *smart* because, among other reasons, they have the ability to extend existing default functionality by installing new mobile applications (*apps*).

3.9.1 Installing *apps*

The user can install new *apps* from official shops or markets, such as Google Play (Android), App Store (iOS) or Microsoft Store (Windows Phone), or from other unofficial third-party repositories or markets (depending on the mobile platform). Some mobile platforms such as iOS allow, by default, the installation of apps coming from the official market (exclusively), so although infection by malicious code can occur, it must first be introduced and propagated in the official market.

Although there have been several cases of malicious code in Apple's App Store, the controls in place mean that the likelihood of infection is lower than on other mobile platforms, and once detected, it is removed from the market as soon as possible (although the mobile devices already infected will remain so).

3. Good practices in the configuration and use of mobile devices

Other mobile platforms such as Android are more flexible and allow, if the user so wishes, the installation of apps from both the official app market and other unofficial markets, as well as directly from web servers or via email messages through attachments [15]. This flexibility is used by attackers to distribute malicious code and infect the devices.

Recently, modern versions of iOS (9 or higher) allow the installation of apps via USB (see section 3.2 “Communications via USB”), a technique known as *sideloading*, as was already the case in previous versions of Android, if the device has an insecure configuration or is not locked (depending on the mobile platform).

With these capabilities in mind, it is important that the user does not install any *app* that does not come from a trusted source , such as official *app* markets.

On mobile platforms that have this flexibility, it is recommended not to enable the functionality that allows the installation of apps from untrusted third-party repositories (unknown sources) and under no circumstances install *apps* from disreputable sources, even if they are free.

It is better to pay the price of an app (between €0.99 and €2.99 for most of them), than to expose all our personal information just to save a few euros.

> **It is important that the user does not install any *app* that does not come from a trusted source, such as official *app* markets.**

---

[15] “Alternative (Open) Distribution Options”. Android Developers. Documentation. https://developer.android.com/distribute/tools/open-distribution.html

3.9.2 App permissions

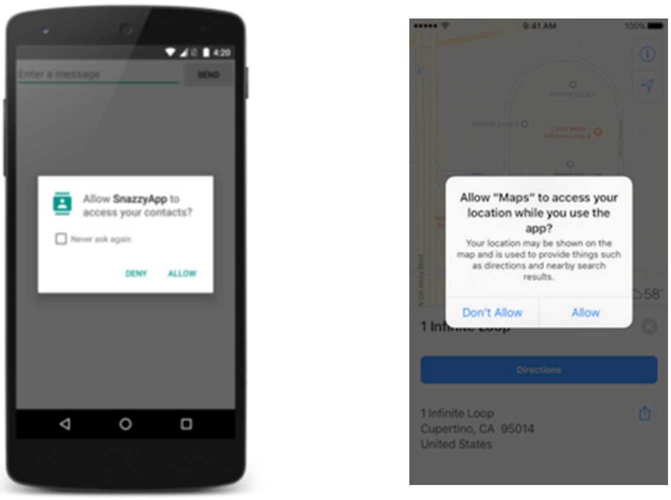
Mobile devices have a restricted execution environment, where an *app* does not have access, by default, to the files and data of other apps or the operating system. To gain access to such data and/or additional functionality, the *app* must request permissions from the user, e.g. to access the user’s contacts, calendar, or hardware components such as the camera or microphone, or photos.

It is recommended not to grant unnecessary or excessive permissions to *apps*, thus limiting the data and functionality to which they will have access .

Depending on the mobile platform and operating system version, permissions will be requested from the user when installing the *app*, or during its execution, or when making use of certain functionality for which a particular permission is required, e.g. an application that allows barcode scanning and requests permission to access the camera.

It is recommended not to grant unnecessary or excessive permissions to *apps*, thus limiting the data and functionality to which they will have access . To do this, it is necessary that the user first understands why an *app* is requesting a particular permission and what the permission is needed for within the functionality provided by the *app*.

Properly developed *apps* should inform the user of the specific reasons for requesting permission.



Allow **SnazzyApp** to access your contacts?

☐ Never ask again

Allow “Maps” to access your location while you use the app?

Your location may be shown on the map and is used to provide things such as directions and nearby search results.

Figure 3-8 Permission requests by apps on Android and iOS. Source: Android Developers[16] and Apple Developers[17]

---

[16] Requesting Permission. Apple Developers. https://developer.apple.com/ios/human-interface-guidelines/interaction/requesting-permission/

[17] Requesting Permissions at Run Time. Android Developers. https://developer.android.com/training/permissions/requesting.html

3.9.3 E-mail

One of the most common tasks for which mobile devices are used is for accessing e-mail, and there is a default *app* for that.

It is recommended to consult the CCN-CERT's email best practice guide[18], as many of the recommendations therein apply not only to traditional computers (such as PCs), but also to mobile devices.

3.9.4 Messaging applications

Additionally, mobile devices are frequently used to establish personal and professional communications with family, friends, acquaintances, colleagues and other work contacts through messaging applications, either by sending and receiving text messages (SMS) or multimedia messages (MMS), or by using other messaging services such as WhatsApp, Telegram, Line, etc.

Through these services it is possible to receive messages with web links containing malicious code, with the aim of infecting and compromising the victim's mobile device. The use of malicious links is one of the most commonly used techniques to execute code on the victim's device or to obtain information from the victim. The type of link (where it points to, what kind of actions it will execute, etc.) will depend on the attackers' objectives.

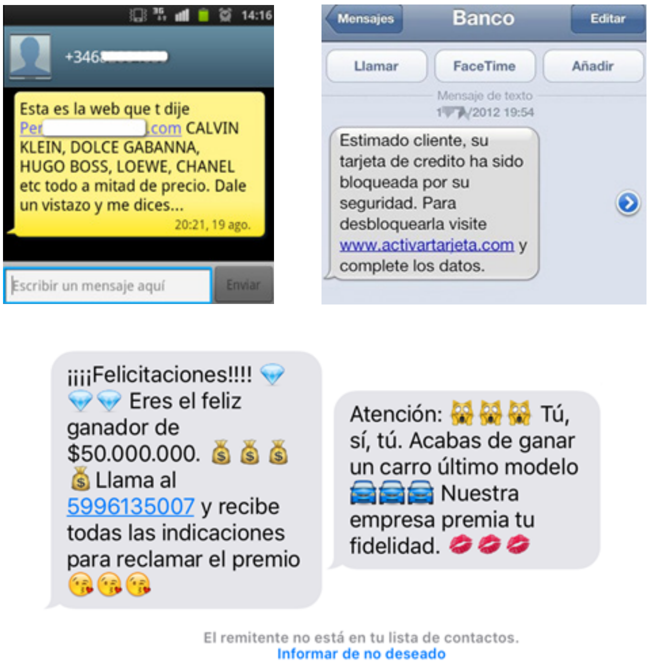
---

18. "Good Practices. CCN-CERT BP-02/16. Electronic mail". CCN-CERT. Report. July 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html

The most common uses of malicious links are described in the CCN-CERT's good email practices guide[19], and apply to messaging communications: phishing, downloading malicious files or *Web Exploit Kits*.

Attacks based on malicious links distributed via messaging apps are often referred to as SMiShing, rather than phishing (the term used for email distribution), and also include messages that are attractive, suggestive or that the user should take urgent action on:

Attacks based on malicious links distributed via messaging apps are often referred to as SMiShing.



Esta es la web que t dije Per[redacted].com CALVIN KLEIN, DOLCE GABANNA, HUGO BOSS, LOEWE, CHANEL etc todo a mitad de precio. Dale un vistazo y me dices...
20:21, 19 ago.

Estimado cliente, su tarjeta de credito ha sido bloqueada por su seguridad. Para desbloquearla visite www.activartarjeta.com y complete los datos.

¡¡¡¡Felicitaciones!!!! 💎💎💎 Eres el feliz ganador de $50.000.000. 💰💰💰💰 Llama al 5996135007 y recibe todas las indicaciones para reclamar el premio 😘😘😘

Atención: 🙀🙀🙀 Tú, sí, tú. Acabas de ganar un carro último modelo 🚘🚘🚘 Nuestra empresa premia tu fidelidad. 💋💋💋

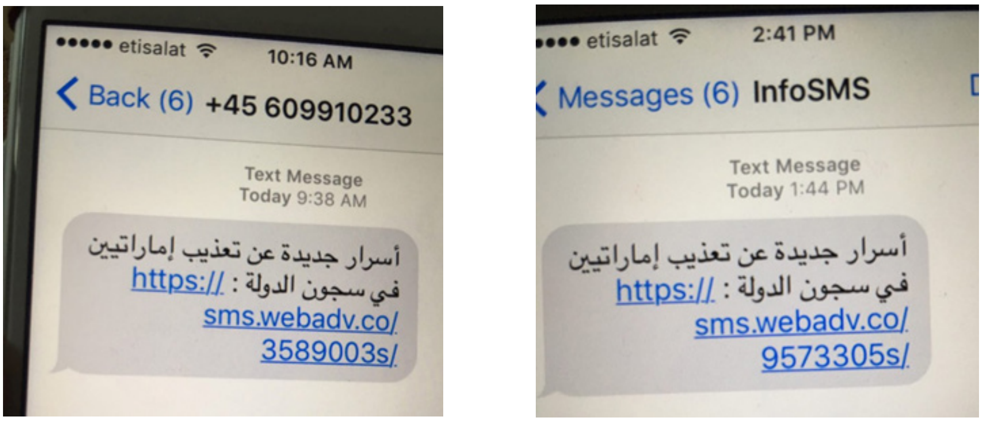
El remitente no está en tu lista de contactos.
Informar de no deseado

Figure 3-9 Examples of SMiShing messages. Sources: OSI[20], Hora Jaén[21], MDE[22].

---

[19] "Good Practices. CCN-CERT BP-02/16. Electronic mail". CCN-CERT. Report. July 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html
[20] https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms
[21] http://horajaen.com/detienen-a-siete-jiennenses-por-una-estafa-de-pishing/
[22] http://descubre.mdeinteligente.co/smishing-5-consejos-para-cuidarte-de-las-estafas-via-mensaje-de-texto/

The attack called Pegasus[23] that took place in August 2016 against Ahmed Mansoor, an internationally renowned human rights defender based in the United Arab Emirates, used these techniques based on sending a malicious SMS message to infect the victim's iPhone and take complete control of it through sophisticated *spyware*, using three new previously unknown vulnerabilities (*0-days*):



Text Message
Today 9:38 AM

أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : https://sms.webadv.co/3589003s/

Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : https://sms.webadv.co/9573305s/

Figure 3-10 Harmful SMS messages received by Mansoor with spoofed sender (Pegasus).
Source: Citizenlab

Undoubtedly, the most effective advice for identifying harmful messages is common sense, just as it is for email. This means **that any anomalous or unusual sign or pattern should arouse the user's suspicion**.

An irregular pattern or sign can mean: receiving a message from an unfamiliar sender, receiving a message requesting personal information, the content of the message being too attractive to be true, etc.

---

[23] "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender". Citizenlab. Blog Post. Agosto 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

For example, a message sent by a trustworthy company that presents an unusual subject or request and includes a link should generate a certain amount of mistrust on the part of the user. In this scenario, the best thing to do before clicking on the link is to contact the supposed sender using a different means of contact, such as telephone, e-mail, etc. In this way, it will be possible to corroborate whether the message received is legitimate or not.

It should be noted that, as with emails, an attacker may sometimes impersonate the sender of the message, so this information should not be blindly relied upon.

3.9.5 Social media

Another very common use of mobile devices by users is the interaction with social networks, such as Facebook, Twitter, Instagram, etc.

When posting any kind of personal information or images on social networks, **it is recommended to assess the sensitivity and privacy of the data to be published and to take into account that such content will potentially be available to many people**, not only to the user's closed circle of friends.

Such information is often used both to coerce or blackmail the user with its dissemination and to obtain critical data or to establish relationships and communications that determine the success or failure of a *spear phishing* campaign against the user or the organization he/she works for.

3.9.6 Web browsing

It is also very common to use mobile devices for web browsing tasks, with the aim of consulting web content or interacting with a multitude of services available on the Internet, using the standard web browser or a specific *app* for its use.

The protocol involved in web browsing for accessing web content and services is HTTP. This protocol has been used since 1991[24] and when it was implemented no security measures, such as encryption or strong authentication of communications, were taken into account.

This means that the entire process of requesting and responding to content between the mobile device and a web server or application is done in plain text, meaning that at any point in the transmission an attacker could view and manipulate the content of web pages.

Due to these shortcomings in HTTP, various technologies and extensions have been developed to incorporate security measures into web communications, for example, to guarantee the encryption of transmitted data. For this reason, the HTTPS protocol was developed, based on TLS, indicating its additional security features with the letter “S”.

Using HTTPS allows, for example, initializing a TLS exchange with the web server prior to sending any sensitive data, such as user credentials needed when accessing a web service like email, social media or a bank or online shop. In this way, an attacker monitoring communications would not be able to access such sensitive information.

---

24. http://info.cern.ch/hypertext/WWW/History.html

In the case of web browsing through a mobile device, such as Safari, Chrome, Firefox, etc., the user has the possibility of indicating that they wish to use the HTTPS protocol, unlike the communications used by mobile applications, where the connection is carried out automatically by the *app*, without the user having to or being able to indicate the server to which they wish to connect or how they wish to connect.

Most well-known providers, organizations and companies with a website allow access to their web servers via HTTPS, although many organizations still use HTTP exclusively.

It is therefore recommended, whenever possible, to make use of the HTTPS protocol by inserting the text "https://" before entering the web address of the server you wish to connect to.

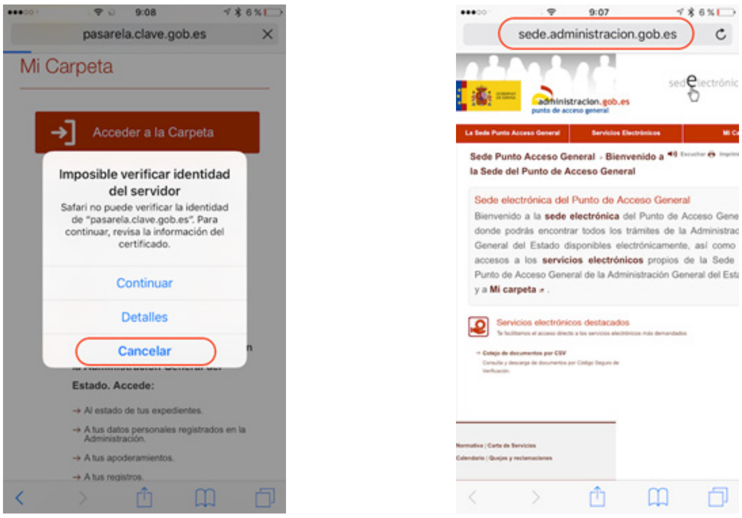
It should be noted that these security measures are susceptible to attack. For example, HTTPS is vulnerable to *Man-in-the-Middle* (MitM) attacks, where the attacker gets in the middle of the communication between the mobile device and the remote web server or application, with the aim of manipulating the communication. On the one hand, the attacker may try to impersonate the legitimate web server or application, offering the victim a digital certificate that may be similar to the legitimate one, but will not be accepted as valid or trusted by his web browser.

As a result, the web browser will generate a certificate error message which, if accepted by the user, will cause an encrypted connection to be established with the attacker, allowing the attacker to intercept all exchanged data, including login credentials and other sensitive and critical information.

On the other hand, the attacker may try to eliminate the use of HTTPS in any communication between the user and the legitimate web server or application, using an attack known as sslstrip, with similar consequences for the user.

The user should never accept an error message from the web browser associated with an invalid digital certificate, and it is recommended to cancel the connection. Instead, you should check whether you are actually connecting to the web server you are trying to connect to via the web address and try to get more details on why the certificate error has been generated.

If a connection needs to be established, it is recommended to make use of another network, e.g. the 2/3/4G mobile data network, if a Wi-Fi network was being used, or even a computer connected to a different network, such as the office or home network.



Imposible verificar identidad del servidor

Safari no puede verificar la identidad de "pasarela.clave.gob.es". Para continuar, revisa la información del certificado.

Sede Punto Acceso General - Bienvenido a la Sede del Punto de Acceso General

Sede electrónica del Punto de Acceso General

Bienvenido a la **sede electrónica** del Punto de Acceso Gene donde podrás encontrar todos los trámites de la Administrac General del Estado disponibles electrónicamente, así como accesos a los **servicios electrónicos** propios de la Sede Punto de Acceso General de la Administración General del Esta y a **Mi carpeta** .

9:08
6 %
pasarela.clave.gob.es
Mi Carpeta
Acceder a la Carpeta
Continuar
Detalles
Cancelar
Estado. Accede:
Al estado de tus expedientes.
A tus datos personales registrados en la Administración.
A tus apoderamientos.
A tus registros.
9:07
6 %
sede.administracion.gob.es
administracion.gob.es
punto de acceso general
La Sede Punto Acceso General
Servicios Electrónicos
Escuchar
Servicios electrónicos destacados
Normativa | Carta de Servicios
Calendario | Quejas y reclamaciones

Figure 3-11 MitM and sslstrip attacks: Certificate error or lack of HTTPS.

To verify whether the connection to a web server or application is encrypted, it should be verified that the address bar of the web browser makes use of HTTPS, indicated by the text "https://" at the beginning of the web address.

Unfortunately, by default, the address bar of modern mobile web browsers tends to minimize the information displayed to the user, highlighting only the domain to which the connection has been established.

In order to get all the details of the web server and the accessed resource, as well as to check if the connection method used is HTTPS (checking the appearance of a padlock is not always enough), it may be necessary to select the address bar and scroll to the left to display all the details:

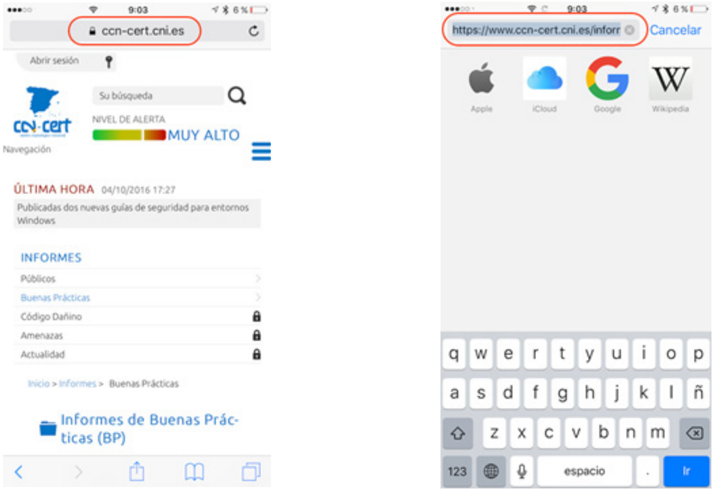


Figure 3-12 MitM and ssltrip attacks: Manual verification of HTTPS usage.

4. Other generic recommendations

From a corporate point of view, it is recommended to make use of enterprise *Mobile Device Management* (MDM) solutions, in order to define, establish and monitor different security recommendations on all mobile devices in the organization in a homogeneous way.

These solutions allow security settings to be applied to mobile devices based on the organization's pre-defined security policies.

The process of *jailbreaking* (iOS) or *rooting* (Android) consists of carrying out certain actions (by intentionally exploiting vulnerabilities) on the mobile device in order to take complete control of it and have maximum privileges.

Although some users perform this process to add functionalities that do not exist by default, due to limitations imposed by the manufacturer, its use is not recommended.

As a result, many of the existing security mechanisms on mobile platforms are disabled. Without sufficient technical knowledge, after *jailbreaking* or *rooting*, the user will have a mobile device that is more insecure and could be more easily compromised or infected.

4. Other generic recommendations

It is recommended to use strong passwords[25] for each and every service and application that is accessed from the mobile device. Such passwords should not be reused between different services or applications.

Additionally, for services or applications that have this functionality, and especially for the most critical ones, it is recommended to use a second authentication factor.

If possible, it is recommended not to store the credentials of the different services and applications used on the mobile device itself, as these could be retrieved in the event of the device being infected.

The organization's security officer should be informed immediately if the mobile device is lost or misplaced, as well as if any abnormal or suspicious behavior is identified when using the device.

In addition to the access code, it is recommended to set the PIN associated with the SIM card to prevent misuse and unauthorized use of telephony communication capabilities, such as making phone calls. The access code and the PIN of the SIM card must be different.

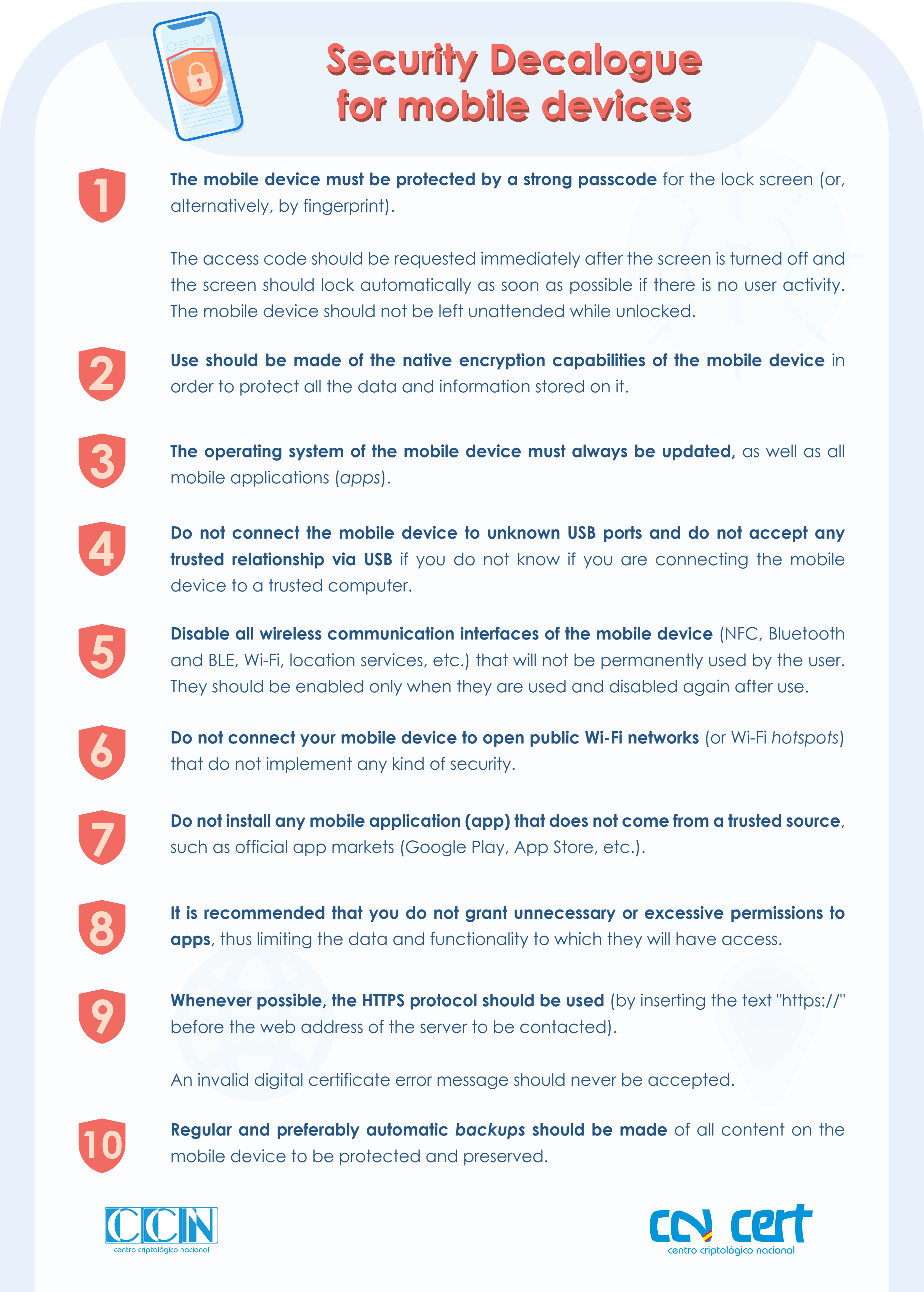
In order to identify possible infections in the mobile device or any other related fraud, the user should check monthly the consumption associated with his contract through the mobile operator's bill and identify as early as possible anomalies, such as the sending of text messages (SMS) or multimedia messages (MMS), or voice calls that he/she does not recognize.

---

[25] **25.** Schneier on Security. Blog Post. March 2014. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

5. Decalogue of recommendations

This decalogue of best practices aims to improve the level of protection and security of mobile devices.



Security Decalogue for mobile devices

1. **The mobile device must be protected by a strong passcode** for the lock screen (or, alternatively, by fingerprint).

   The access code should be requested immediately after the screen is turned off and the screen should lock automatically as soon as possible if there is no user activity. The mobile device should not be left unattended while unlocked.

2. **Use should be made of the native encryption capabilities of the mobile device** in order to protect all the data and information stored on it.

3. **The operating system of the mobile device must always be updated,** as well as all mobile applications (*apps*).

4. **Do not connect the mobile device to unknown USB ports and do not accept any trusted relationship via USB** if you do not know if you are connecting the mobile device to a trusted computer.

5. **Disable all wireless communication interfaces of the mobile device** (NFC, Bluetooth and BLE, Wi-Fi, location services, etc.) that will not be permanently used by the user. They should be enabled only when they are used and disabled again after use.

6. **Do not connect your mobile device to open public Wi-Fi networks** (or Wi-Fi *hotspots*) that do not implement any kind of security.

7. **Do not install any mobile application (app) that does not come from a trusted source**, such as official app markets (Google Play, App Store, etc.).

8. **It is recommended that you do not grant unnecessary or excessive permissions to apps**, thus limiting the data and functionality to which they will have access.

9. **Whenever possible, the HTTPS protocol should be used** (by inserting the text "https://" before the web address of the server to be contacted).

   An invalid digital certificate error message should never be accepted.

10. **Regular and preferably automatic *backups* should be made** of all content on the mobile device to be protected and preserved.

CCN centro criptológico nacional

CCN cert centro criptológico nacional

Figure 5-1. Security Decalogue

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es