MOBILE DEVICES SECURITY GUIDEBOOK

CAIS

RNP

Tablets and smartphones are everyday more present in peoples' lives. In contrast with personal computers, these mobile devices have less processing power, less memory capacity and different user-interaction interfaces. We must also adopt alternative strategies in these devices to protect the user against security threats.

CAIS/RNP wrote this guide to help you with mobile devices, providing simple and effective tips for operating them more securely.

These tips may be used on many operating systems such as iOS (Apple iPhone 3GS and above, iPad) or Android variants.

SECTION 1
IN THE CORPORATE ENVIRONMENT

Blackberry is the platform with the best security resources for corporations.

- **For many years RIM (device manufacturer) has been offering solutions for device remote management** via the BlackBerry Enterprise Server, known as BES. The system admin may, among other things, use this service to force strong passwords, block Wi-Fi connections, and prohibit installation of apps from social networks.

- **Encryption support in BlackBerry is widely recognized as the best**, from secure data transfer to secure storage, all this already available in the device with no extra installation requirements.

Google Android and Apple also provide features for remote administration of corporate devices.

- **iOS Security – Mobile Device Management (MDM)**
  http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf

- **Device Policy Administration for Android**
  http://support.google.com/a/bin/answer.py?hl=en&answer=1056433

SECTION 2

TIPS POR ONLINE SHOPPING

Prefer the mainstream smartphone operating systems. Currently, main options are Google Android, Apple iPhone, and recently Windows Phone.

Historically, there have been more security incidents with malicious apps in Google Android than in Apple iPhone / iPad – the market dominant systems. Although this favors Apple devices, beware that no system is free of security threats.

If possible, contract manufacturer/reseller insurance or extended warranty. These are some of the options available in Brazil:

- *http://www.pitzi.com.br*
- *http://www.portoseguro.com.br/seguros/seguro-para-equipamentos-portateis*
- Avoid giving personal / financial data to websites without SSL / TLS (secure protocol). This tip is especially important when you use Wi-Fi connections (802.11a, 802.11b, 802.11g, 802.11n). To check if a website provides a secure connection look for the image of a lock in the browser's status bar. Alternatively, check if the web address begins with https://. The "s" at the end of "http" means that the server is using the SSL / TLS protocol.

- If possible, avoid using any application that handles personal data on open Wi-Fi networks - those networks do not request passwords for connection and are usually available at airports and coffee shops. Some examples of applications you should avoid with this type of connection are bank and online shopping apps.

ARE YOU AWARE?

- It is possible to request a two-step authentication to your Gmail account. For this, set the 2-step verification option in your google account at:

  https://accounts.google.com/b/0/SmsAuthConfig

- Google also offers the app "Google Authenticator". However, we suggest using the SMS security verification because it works even when the device's battery is discharged.

- We recommend you register a secondary mobile phone number (option "backup phones") in case your primary mobile phone cannot receive SMS for some reason.

- We recommend you keep a printed copy of the "backup codes". These are emergency passwords Google works with if you do not have access to the phones registered to receive the security SMS.

SECTION 3

IN CASE OF THEFT OF YOUR SMARTPHONE OR TABLET

First of all, understand that **your major priority is to safeguard your personal information**.

There are minimal chances of recovering your lost or stolen device in Brazil, so prepare yourself to lose it without major impacts on your personal / professional life.

iPhone and iPad devices have a feature that locates the lost / stolen device. You also have the option to block the device, erase all data or just send a message (with great emphasis) to the phone. Refer to the item 2.2 (Search iPhone) for more information.

Android devices provide several ways to locate and perform actions on your lost or stolen device. One choice is Android Lost (*http://www.androidlost.com*).

You may prohibit your lost or stolen smartphone to access social networks. You can do it remotely. Some examples:

- **Twitter:**
  https://twitter.com/settings/applications

- **Facebook:**
  https://www.facebook.com/settings?tab=applications

- **Gmail:**
  https://accounts.google.com/b/0/IssuedAuthSubTokens

SECTION 4
PREVENT ACCIDENTS

SYNCHRONIZATION. Synchronize your smartphone or tablet contacts and calendar data. This way you will not lose contact info in case of loss, theft or damage. The major Webmail services (e.g. Gmail) support synchronization features easily.

BACKUP! All systems offer the option of full device backup. This is usually done automatically (iPhone, BlackBerry) as you connect the device to your personal computer to sync multimedia, contacts and apps.

VPN. Smartphones have the option to connect via 3G, which is more secure against spoofing than using an open Wi-Fi network. However, we also recommend VPN connections, which create secure channels of communication, even when the network used to access the Internet is not secure. For more information, please refer to section 5 (Laptops).

ANTIVIRUS. Install or not? The incidence of virus in smartphones is not alarming yet, but significant enough - particularly on Google Android - that people are starting to treat viruses in smartphones as they do in personal computers.

- Security solutions do not only deal with viruses.
- Some functionalities are redundant (e. g. location, blocking / deleting data remotely).

- Follow some product recommendations. We'll point to single solution to avoid bias::

  - **F-Secure Mobile Security**
    http://www.f-secure.com/pt/web/operators_global/security-services/protection-for-mobile/overview

  - **Kaspersky Mobile Security**
    http://brazil.kaspersky.com/produtos/produtos-para-usuarios-domesticos/mobile-security

  - **McAfee Mobile Security**
    http://home.mcafee.com/store/mobile-security

  - **Trend Micro Mobile Security**
    http://br.trendmicro.com/br/products/enterprise/mobile-security/

INSTALL APPS ONLY FROM OFFICIAL RELEASE SOURCES

iPhone and iPad allow you to install apps from alternative sources only if your device is jailbreak. Otherwise, you are prevented from accessing unofficial sources, therefore guaranteeing app authenticity.

Official release sources for each platform:

- **Android:** Google Play
- **iPhone / iPad:** Apple iTunes App Store
- **BlackBerry:** BlackBerry App World

IOS
(IPHONE/IPAD)

iOS is the operating system of several Apple devices: iPhone (3GS and newer), iPad (all versions) and Apple TV. The version considered in the following tips is iOS 5.1.1, released in May 2012.

All tips below refer to the Settings app, available in all iOS devices.

We consider only non-jailbreak devices, i.e. iPhone or iPad devices with the original iOS operating system from Apple. To check if your device is unlocked (if it is jailbreak) look for the Cydia app - if this app is present, then your device has been unlocked.

1. General

1.1 Software updates

- Choose the option “Software Update” and search for new iOS updates. WARNING: If you have a jailbreak device the update process will restore the original SW restrictions in your device.

1.2 Automatic lock

- We recommend setting the auto-lock option to “2 minutes” - a good choice for both usability and security.

1.3 Passcode lock

With this option, several lock features can be defined:

- Simple passcode: check this option for simpler passcodes, best suited for iPhone.
- With this option checked, the passcodes will be 4-digit numbers. For more complex passcodes, disable the option "Simple Passcode". We recommend this setting for corporate iPads and iPhones.
- Select "Delete Data" to strengthen the protection of information in your device. This option is useful in case your device is lost or stolen. If a person enters the wrong passcode 10 times, the data in your device will be fully erased automatically.

2. ICLOUD

iCloud is a cloud computing and storage service whose operations started in October 2011. Basically, this is a feature Apple offers to synchronize all iOS devices (Apple TV, iPhone 3GS and the newer iPad) and personal computers (Mac OS X starting on version Lion).

iCloud features include calendar syncs, contacts syncs, full device backup, browser bookmarks sync. **More information at: *http://www.apple.com/br/icloud/*.**

2.1 Documents and data

- This option is useful as backup of stored documents and apps installed in your device.

2.2 Search iPhone

- This feature allows you to search for an iPhone, iPad or Macbook (with Mac OS X Lion version or higher).
- Assume that recovering the device in case of theft is not always feasible. However, losing data and allowing a stranger to access your information is even worst.
- This feature allows you to remotely erase all data on the device. This is done from the following website:

  https://www.icloud.com/

- **CAUTION:** If the credentials (Apple ID) are stolen, you can not only locate the device as completely erase all data from the icloud.com website. Choos complex passcodes for your Apple ID, and "security questions" that cannot be answered easily.
- In order to change your Apple ID passcode, log in to the website below and choose the option "Password and security":

  https://appleid.apple.com/

- Change the passcode by selecting "Change Password" (section "Choose a new password"). We recommend you choose your own security question.

2.3 Storage and backup

- Use this feature to back up your device data in the cloud. This feature replaces the backup process running when Apple iTunes opens, after USB port connection.

3. Phone

- Set a passcode for the SIM card.
- Every time the phone boots or the chip is inserted in the SIM slot, a passcode will be requested.
- Choose the option “SIM PIN”. Set a new PIN code by first checking the standard PIN code given by the carrier who provided the SIM card. For example, the standard PIN code for VIVO-BR is 8486 and 1010 for TIM-BR.

ANDROID
(SMARTPHONES AND TABLETS)

The main security settings for Android systems are in the section “Security” of “System Settings” (access through the Menu button).

- **1. Screen lock**
  - Select one of the screen lock options. We suggest the “Password” option, which allows more complex passwords.
  - Options “PIN” (a number) and “Standard” (joining points forming a certain pattern) are less recommended because they are less complex.
- **2. Configuration of SIM Lock**
  - Check the option “Lock SIM card”
  - Modify the PIN code (usually the standard code defined by the carrier) by choosing the option “Change SIM PIN”

- **3. Unknown Sources (under Device Administration)**

  - One of the biggest problems in the Android platform is the growing number of malicious apps which have already been found. Unfortunately, a malicious app is not easily identified by the user. Malicious apps are often identified by security experts, reporting to Google, who then removes the service. Our recommendation is simple: always use the official service for application releases - Google Play – at: *http://play.google.com*.

  - Uncheck the option "Allow installation of applications from unknown sources." Thus, only applications authorized by Google Play can be installed.

BLACKBERRY
(RIM)

As with Android, there are several versions of RIM's operating system for smartphones. The current versions of new devices are BlackBerry OS 6 and BlackBerry OS 7, but there are still many devices with BlackBerry OS 5 on the market.

The follow items are the essential security settings in Blackberry smartphones, regardless of which OS version. Look for the "Settings" option.

- **PASSWORD.** Define a password for you BlackBerry.

- **SECURITY OPTIONS.** This section has the most essential security items on a BlackBerry. The most important of which is:

  ENCRYPTION. Enable encryption both in main memory and in the memory card (SD / MicroSD). Choose at least the "Strong" password strength.

- **More information at :**

  http://docs.blackberry.com/pt-br/smartphone_users/?userType=1

SECTION 5
LAPTOPS

You have already attended many talks on PC security and read many guidelines in the past DISI events. It does not hurt to remember some key points on the mobile security of laptops, netbooks and ultrabooks and the risks involved in Wi-Fi networks.

- **Install anti-virus software and keep it updated.** Some operating systems have more exploits than others for their popularity, but keep in mind that none of them is free from infection.

- **Install a personal firewall and keep it updated.** More important than installing the firewall is to understand how this security tool works. Owning a firewall and carelessly clicking "OK" for all alerts is not a secure behavior.

- **Keep all software updated, but pay special attention to the web browser.** The browser is the main gateway for security threats. It is extremely important that you keep Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera or any other browser always updated.

- **Always use licensed, original software on your computer.** Usually, manufacturers make security updates more difficult to computers with unlicensed software.

- **Updating software and Operating Systems (Microsoft Windows, Apple Mac OS X, any GNU / Linux distribution) regularly is very important** in protecting against exploitation of known and fixed security vulnerabilities.

- **Avoid using open Wi-Fi networks.** You already know you should always use SSL / TLS for secure connections to websites. The problem is that usually there are countless applications that access the Internet and they do not always do it with the SSL / TLS protocols. If possible, use a 3G link or use a VPN.

- **A VPN is very useful to secure an open Wi-Fi network or a wired hotel network.** There are many contract options for VPNs, some good choices are given in the following article:

  Five Best VPN Service Providers
  http://lifehacker.com/5759186/five-best-vpn-service-providers

- **BEHAVIOR.** Avoid opening e-mail links, particularly those received from organizations or people you do not know

SECTION 6

MEMORY CARDS AND USB STORAGE DEVICES

SD memory cards and USB storage devices ("flash/pen drives" and external hard drives) are very common nowadays. **The storage capacity of these devices is very high and this requires careful attention.**

- **We know it's tempting to use a flash drive as a destination for your backups, but we suggest you don't do it. There is a considerable chance of loss or theft.** Moreover, failures while removing the flash drives or even accidental power outages during writes can cause data losses. Prefer external hard drives, a NAS (Network-attached Storage) or even a backup service in a secure cloud.

- **Add your flash drive or memory card mount point to the scan paths of your anti-virus software.**

- **Encrypt the data in your memory card (if it is not for use in digital cameras) and flash drive such that the data stored are not readable by third parties in the event of loss or theft**. Again, remember that information is your most valuable asset. We suggest using TrueCrypt (http://www.truecrypt.org), which is compatible with all major operating systems in the market.

SECTION 7

HOW TO DISCARD OLD MOBILE DEVICES SAFELY

You have been using your smartphone for years and now it is time to discard the old model. **What to do before you give it a new destination; either sell it or donate it?**

Below, we offer some basic tips for the safely disposing your mobile devices:

- **Smartphones and tablets store many different types of data.** We may argue these devices store a wider variety of personal data than personal computers, particularly personal photos. You must ensure these data are not readable by unauthorized people.

- **The first and most important action you must take is to clean up all user data/configurations and cached information in the device.** This procedure has different names depending on the manufacturer such as data wipe, data reset, master clear, factory restore, redefine.

- How to clean up each device:

  - **iPhone / iPad:**
    Go to app "Settings", option "General", option "Redefine" (the last option in the General screen). Choose the option "Delete All Content and Settings".

- **Android:**
  On "Menu" button, option "System Configurations", option "Backup and Restore". Choose the option "Restore Factory Configuration".

- **BlackBerry:**
  - In the home screen or in a folder, click on the icon Options.
  - Click on Security Options and then click on General Configurations.
  - Press Menu key.
  - Click on Clean up mobile device.
  - To remove all third-party apps from the device, check the box Include Third-Party Apps.
  - Click Continue.
  - Type blackberry.

TIPS

Except for the iPad and iPhone devices, most smartphones and tablets have the capability to expand storage with SD or MicroSD memory cards. The expansion card slot is usually located on an external port or behind the battery. Before donating or selling this device, make sure the memory cards are clean (photos, system files, documents).

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL

BRASIL

PAÍS RICO É PAÍS SEM POBREZA