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).