



## TIP SHEET SERIES NO.22

# Securing Mobile Devices

Mobile devices (smartphones, laptop computers, and tablets) are always available to you everywhere you go, and are used for business, travel entertainment, or for different purposes. These devices allow you to easily connect to the world around you. However, within these devices, you carry many information such as people, photos, videos, locations, health and financial data. In this context, it is very important to use your portable devices safely.

### ■ **Protect Your Personal Information**

**Secure Your Devices:** Use strong passwords while locking your devices or take advantage of your device's touch identity features. In this way your device will stay away from prying eyes and your information will be preserved in situations such as lost or stolen.

### ■ **Be careful about Applications**

Think once again about who and how this information is collected through applications.

### ■ **WiFi and Bluetooth must be disabled if not used.**

Some stores and various places watch with Wi-Fi or Bluetooth in their coverage area. WiFi and Bluetooth must be disabled if not used.

### ■ **Be Informed About WiFi Points**

Public wireless networks and mobile data sharing points are not secure. A malicious person connected to them can see what you are doing potentially in your mobile device. In this context, limit what you want to do on public open WiFi networks, especially avoid accessing important accounts such as email and financial services. If necessary, you should use a virtual private network (VPN) or personal / mobile hotspot.

### ■ **Your machine should be clean**

**Keep Your Mobile Devices and Applications Up-to-Date:** Your mobile devices are as vulnerable as your PCs or laptops. One of the best defenses against viruses, malware and other online threats is the latest security software, web browsers and operating systems.

### ■ **Delete When Your Work is Over**

We reduce most of our applications to specific goals such as "vacation planning" and then we do not need these applications. There may also be a lot of applications that are needed in the future and not used at the moment. For this reason, it is a good security measure to delete all applications that you do not use.