CONNEXIS CASH

MOBILE SECURITY

AWARENESS & GOOD PRACTICES

BNP PARIBAS

The bank for a changing world

BNP Paribas provides you with some tips and good practices to help you in keeping your mobile devices as secure as possible

Mobile Protection

Access Protection

- **Consider using a screen lock** as the first security step in order to protect the mobile device
- **Configure an automatic terminal lock** after 5 minutes of maximum non-activity
- **Limit the number of unlock attempts**, then set a longer lock time as well as an automatic erasure after a dozen of failed attempts
- **Do not leave the terminal unsupervised**. A temporary access to a mobile may be sufficient to be compromised without the user being aware even when it is locked
- **A screen lock is helpful but it cannot prevent someone from removing the SIM card** from the phone and use it on another phone
- **To anticipate this risk, the set-up of a SIM card lock in the form of a PIN number** has to be entered when a phone is turned on in order to connect to a network
- **Do not connect the device to an uncontrolled workstation or any other device that is not trusted.** This would establish an uncontrolled direct connection

Remote Tracker

- **Remote tracking can be activated if the phone is lost**
- **Disable a phone if needed** by using '**Find my Device**' on Android or '**Find my iPhone**' on Apple iPhone functionalities

Application Security

- Applications must have strictly **sufficient permissions** to their functions, whether it is for data access or the internet, but also for control of various sensors. The permissions granted must be checked at least during their **installation** and at each update to ensure that they have not been changed
- **Applications must be updated regularly and quickly as security patches are offered**

Network Access

Wi-Fi Usage

- **Only use the trusted Wi-Fi networks or service providers**
- **Always use a security protection** such as Wi-Fi Protected Access (WPA), if possible
- **Always switch off your wireless connection when it is not in use.** It ensures that people cannot connect to a device without your knowledge and control. It is also worth checking your phone's network security settings as it might be configured to automatically connect to a network when in range without your knowledge
- **Ensure that your home wireless router is protected by a pass code**
- If you are using a mobile wireless or a hotspot, be careful of any malicious connections that look very similar like a legitimate hotspot from a large company
- For sensitive actions, it is better to use a 3G or 4G connection instead, which is much more secure

Bluetooth

- **Bluetooth** is not generally seen as a risk as it has a relatively shorter range (10 metres approximately).
  However, hackers have been known to remotely access a phone if they are in range
- Ensure that your Bluetooth is turned off when it is not in use. Set the Bluetooth configuration to 'non-discoverable', so that people searching for nearby devices cannot find your devices
- Any unknown requests that pop up through a Bluetooth connection, such as an offer to "pair with a device" should be ignored or declined. A hacker in range could make use of your device through a Bluetooth, if it is not secured

VPN Access

- **A Virtual Private Network (VPN)** is a software that can mask the device's location or log on to sites as if the device is based in another country
- Free VPNs are dangerous for different reasons:
  - Malwares can be hidden and steal the data. This can also be used to hijack the accounts and steal money
  - VPNs can also **hijack** the web browsers by redirecting to other malicious sites without permission
- As a result, VPN must be used carefully and it is usually better to use well-known and reputable VPN providers and pay them. Even if it is paid, it does not guarantee the security

Geolocation

- Many smartphone social networking apps automatically upload photos to the internet as many phones are embedded with location tags, also called **'geotags'**, right into the photo files
- Anyone with the right software can look at Facebook or Flickr pictures and find out where people have been and are right at that moment
- Access to the geolocation service must be prohibited for applications whose geographical position functions are not used. If this option is not available in the terminal question, the geolocation service should be switched off when it is not used

Operating System Update

- **Smartphone brands regularly make tweaks and changes to their mobile software.** This is not just for adding new functionalities but also these updates often contain important security fixes that protect the data and devices from hackers
- **Any terminal that can no longer support the evolutions of the operating system should be replaced**

Protection of Data

Data Protection

- It is a wise decision to minimize the information stored on the mobile device as it is easy to lose such a type of device. The option of using external hard disc to store information is safer
- **When the mobile device has to be repaired, it is important to remove the memory card before giving out the mobile device**
- Any exchange of sensitive information must be done in an encrypted form to ensure a privacy and integrity of point-to-point data

Anti-Virus

- The capabilities of smartphones are approaching those of a PC, but most people have no form of protection, although they can face similar threats
- **Spam containing malware attachments or links to attack sites or infected apps that exploit weaknesses in the operating system are all starting to appear**
- Many anti-virus companies now offer free versions of their commercial mobile products and also protection for multiple PCs and phones for a yearly subscription
- Unfortunately, fake anti-virus software designed to infect the device or make people think it is protected are actually not providing a complete protection