2/ Basic Device Security

Easy steps for big improvements in digital security

Every attempt to gain access to information starts with the simplest possible means. So, you have to have “the basics” consistently covered.

DO THE FUNDAMENTALS

- Use a **strong passcode or password** for mobile phones.
- Switch on **disk encryption** on phones, tablets, and computers where possible.
- Strengthen the security and privacy settings of apps, in particular messaging apps, and switch on **PIN or password protection** for apps where possible.
- Protect your computer and user accounts with **strong passphrases.**
- Switch off **Bluetooth and Near-Field-Communication** when not using them.
- Turn off **location services** when not needed.
- Ensure that important and sensitive data is **backed up**.
- Use a **USB-Charge-Only dongle** to prevent unwanted data-transfers while charging.

PROTECT YOUR DEVICES

- Know **where** your devices are at all times.
- Leave them **protected** in the office or in a hotel room if it is safe to do so.
- Place **tamper-evident tape** over the USB ports and hard drive cover.
- Use a **security cable** (Kensington lock) to protect your computer when you work outside the office.

AVOID MALWARE

- Install **anti-malware** applications and keep them updated.
- Exercise caution when opening unexpected attachments, and use **secure file transfer methods** where possible.
- **Update** your apps and operating systems and respond to notifications about updates.
- Download software updates from **original download sources** regularly.
- Download apps from **trusted repositories** like the Google Play Store, F-Droid, or Apple’s App Store only.

MANAGE YOUR APPS

- Use a **privacy-respecting browser** to access social media sites on any device containing sensitive information. Avoid installing social media apps as they often collect sensitive information from your device.
- Customise the **permissions** of apps regularly in the device’s settings.
- **Switch off** apps that you are not using, and **delete** those you do not need. They might run in the background and collect user data.