

BACK TO BASICS

DIGITAL HYGIENE RULES FOR MOBILE PHONES

In the context of the proliferation of threats targeting mobile phones, ANSSI recommends adopting the following 10 best practice rules for using mobile phones :

- **Systematically update your operating system and applications as soon as possible.** Regularly restarting your device can also limit the impact of non-persistent compromises.
- **Activate the operating system's hardening mechanisms** (ie. the [Lockdown Mode](#) in the iOS environment), particularly for high-risk populations.
- **Never connect your digital devices to unknown equipment** (chargers, storage devices, computers, etc.) or to **public Wi-Fi networks**.
- **Uninstall and/or disable unused applications and features.** Also, limit the applications' permissions.
- **Disable wireless interfaces** such as Wi-Fi, Bluetooth, NFC, and location services when not in use.
- **Maintain a strict separation between personal and professional use.**
- **Completely turn off your devices** when you need to leave them unattended.
- **Remove all digital devices from offices and meeting rooms before sensitive conversations** to avoid audio capture. Remember, airplane mode does not prevent spyware from functioning.
- **Avoid exchanging sensitive information via SMS and prefer messaging apps** that use end-to-end encryption to ensure the confidentiality of your exchanges.
- **Be vigilant about phishing messages**, which can disguise illegitimate requests to associate new devices with a messaging account. **If any doubt exists, confirm as far as possible the origin and the legitimacy of the message.**

To go further, see CERT-FR's report
[Mobile phones : Threat landscape since 2015](#)

If you receive alerts (emails, SMS, etc.) from solution providers warning of a potential compromise of an account or device, **contact CERT-FR** by email at cert-fr@ssi.gouv.fr or by phone at **3218** (free service + cost of a call) or +33 (0) 9 70 83 32 18.