

LES ESSENTIELS

HYGIÈNE NUMÉRIQUE DES TÉLÉPHONES MOBILES

Dans un contexte de prolifération de menaces ciblant les téléphones mobiles, l'ANSSI préconise d'adopter ces dix règles de bonnes pratiques dans l'utilisation de ces équipements :

- Mettre à jour systématiquement et dans les meilleurs délais le système d'exploitation de vos équipements ainsi que leurs applications. Un redémarrage régulier permet également de limiter les impacts d'une compromission non persistante.
- Activer les mécanismes de durcissement du système d'exploitation, notamment pour les populations à risque. Le « [mode Isolement](#) » (lockdown mode) en environnement iOS en est un exemple.
- Ne jamais connecter vos équipements à un appareil inconnu (chargeur, support de stockage, ordinateur, etc.) ou à des réseaux Wi-Fi publics.
- Désinstaller les applications et désactiver les fonctionnalités non utilisées. En complément, limiter les autorisations accordées aux applications.
- Désactiver les interfaces sans fil telles que le Wi-Fi, le Bluetooth, le NFC et la localisation si elles ne sont pas en cours d'utilisation.
- Appliquer une séparation stricte des usages personnels et professionnels.
- Éteindre complètement vos équipements lorsque vous êtes amenés à vous en séparer.

→ Sortir tout équipement numérique des bureaux et des salles de réunion en amont de conversations sensibles afin d'éviter une captation sonore. Pour rappel, le mode avion n'empêche pas un logiciel espion de fonctionner

→ Éviter l'échange d'informations sensibles par SMS et préférer des messageries utilisant un chiffrement de bout en bout afin de garantir la confidentialité de vos échanges.

→ Rester vigilant sur la réception de messages d'hameçonnage, pouvant notamment dissimuler des demandes illégitimes d'association de nouveaux appareils à un compte de messagerie. En cas de doute, confirmer autant que possible l'origine et la légitimité du message.

En cas de réception de signalements (courriels, SMS...) issus des éditeurs de solutions et avertissant d'une potentielle compromission d'un compte ou d'un appareil, **contactez** le CERT-FR par courriel à l'adresse cert-fr@ssi.gouv.fr ou par téléphone au 3218 (service gratuit + prix d'un appel) ou +33 (0) 9 70 83 32 18.