

Sécuriser les smartphones et tablettes pro

Le bureau tient dans la poche — les données de l'entreprise aussi. Les règles pour ne pas les perdre avec.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/smartphones-professionnels

Emails, fichiers, applications bancaires, codes de double authentification : le smartphone concentre l'essentiel des accès de l'entreprise. Perdu, volé ou compromis, il ouvre bien plus de portes qu'un ordinateur — et il sort du bureau tous les soirs.

1. Les fondamentaux

- Verrouillage systématique : code à 6 chiffres minimum, empreinte ou visage
- Chiffrement activé (par défaut sur iOS et Android récents — vérifiez sur les anciens)
- Mises à jour du système et des applications appliquées sans tarder
- Applications installées uniquement depuis les stores officiels
- Localisation et effacement à distance activés (Localiser mon iPhone / Localiser mon appareil)

2. Séparer le pro du perso

Le mélange des usages est le vrai risque : une application douteuse installée pour un enfant, un compte cloud personnel qui synchronise les photos de documents... Deux approches selon la taille de l'entreprise : fournir des téléphones professionnels dédiés, ou encadrer les téléphones personnels avec un profil professionnel séparé (Android Enterprise, partition gérée iOS) que l'entreprise peut effacer sans toucher au reste.

Au-delà de quelques appareils, un outil de gestion de flotte (MDM) permet d'imposer le verrouillage, de pousser les mises à jour et d'effacer un appareil perdu en quelques clics.

3. Les pièges en mobilité

- Wi-Fi publics : préférer la 4G/5G, ou un VPN si le Wi-Fi est inévitable
- Bornes de recharge USB publiques : utiliser sa propre prise secteur ou un bloqueur de données
- SMS et QR codes frauduleux : mêmes réflexes que pour le phishing par email
- Bluetooth et partage de connexion laissés ouverts en permanence

4. En cas de perte ou de vol

- Verrouiller puis effacer l'appareil à distance sans attendre
- Faire opposition sur la ligne auprès de l'opérateur (blocage IMEI)
- Changer les mots de passe des comptes connectés sur l'appareil
- Prévenir le référent informatique : les accès professionnels doivent être révoqués
- Déclarer le vol aux forces de l'ordre

L'essentiel à retenir

- 01 Imposer verrouillage et chiffrement sur tout appareil accédant aux données pro
 - 02 Activer la localisation et l'effacement à distance
 - 03 Séparer les usages pro et perso (appareil dédié ou profil géré)
 - 04 Déployer un MDM au-delà de quelques appareils
 - 05 Écrire la procédure perte/vol et la faire connaître
-

Questions fréquentes

Un iPhone est-il plus sûr qu'un Android en entreprise ?

Les deux écosystèmes atteignent un bon niveau... à condition d'être récents et à jour. La vraie fracture n'est pas iOS contre Android, mais appareil maintenu contre appareil qui ne reçoit plus de mises à jour — et usage encadré contre usage libre. Un Android récent géré par MDM protège mieux qu'un vieil iPhone jamais mis à jour.

Les antivirus pour smartphone servent-ils à quelque chose ?

Sur iOS, leur intérêt est marginal (l'architecture limite ce qu'ils peuvent voir). Sur Android, une protection sérieuse peut filtrer les applications et liens malveillants. Dans les deux cas, les fondamentaux comptent davantage : mises à jour, stores officiels uniquement, et vigilance sur les permissions demandées par les applications.

Un collaborateur refuse le profil professionnel sur son téléphone personnel. Que faire ?

C'est son droit — et c'est l'occasion de clarifier la règle : l'accès aux données de l'entreprise depuis un appareil personnel implique un minimum d'encadrement. L'alternative est de fournir un appareil professionnel, ou de limiter l'accès au strict nécessaire via le navigateur, sans synchronisation locale.

Que voit l'employeur via un MDM sur un téléphone personnel ?

Avec un profil professionnel (Android Enterprise, partition iOS), l'employeur ne gère et ne voit que le conteneur professionnel : ses applications, ses données, sa politique de sécurité. Photos, messages et applications personnels restent invisibles — et l'effacement à distance ne touche que la partie professionnelle. Documentez-le noir sur blanc pour rassurer les équipes.

Pour aller plus loin

Cybermalveillance.gouv.fr — sécuriser ses appareils mobiles — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

CNIL — BYOD : quelles sont les bonnes pratiques ? — www.cnil.fr/fr/byod-queelles-sont-les-bonnes-pratiques

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr