Je protège mon téléphone pro.

Je renforce ma sécurité

Je protège ma vie privée

.ubik | infoSEC

Protéger les informations qui comptent pour vous.

Si tu exposes ton téléphone intelligent professionnel aux hackers, tu t'exposes à plusieurs risques sérieux, notamment :

1. **Vol de données sensibles**
   Accès aux emails, documents confidentiels, identifiants de connexion, données clients ou projets stratégiques.

2. **Usurpation d'identité**
   Les hackers peuvent utiliser le téléphone pour envoyer des messages ou emails frauduleux en se faisant passer pour l'employé.

3. **Installation de logiciels malveillants (malwares)**Ceux-ci peuvent espionner les activités, voler des informations, ou servir de porte d'entrée pour attaquer le réseau de l'entreprise.

4. **Atteinte à la réputation professionnelle**
   En cas de fuite d'informations ou de compromission, l'employé peut être tenu responsable, ce qui impacte sa crédibilité et son emploi.

5. **Sanctions disciplinaires ou légales**
   Le non-respect des règles de sécurité peut entraîner des mesures internes voire des poursuites en cas de négligence grave.

En résumé, la sécurité du téléphone intelligent professionnel est cruciale pour protéger à la fois les intérêts de l'entreprise et ta carrière.

Responsabilité
de l'entreprise

a'
.

a1 **Enrôlement d'appareil**
- Utiliser des solutions de suppression à distance (via MDM ou gestion IT) en cas de perte ou vol pour protéger les informations confidentielles.
- Prévenez immédiatement votre service IT en cas de perte ou vol.

a2 **Sauvegarder régulièrement**
- Utilisez une solution de sauvegarde sécurisée fournie par votre entreprise pour garantir la confidentialité et l'intégrité des données.
- Planifiez des sauvegardes automatiques régulières afin de ne jamais perdre vos informations importantes en cas de panne ou de perte.

a3 **Mettre à jour régulièrement**
- Activez les mises à jour automatiques du système et des applications. Installez uniquement les mises à jour officielles.

a4 **Utiliser un antivirus ou une solution MDM**
- Certains employeurs fournissent un logiciel de gestion des appareils mobiles (MDM).
Cela permet de séparer les données pros et perso, et de localiser/effacer l'appareil à distance.

Responsabilité
de l'employé

b'

b1 **Sécuriser l'accès à l'appareil**

- Activez un code PIN, mot de passe, empreinte digitale ou reconnaissance faciale.
- Évitez les codes évidents (ex. : 1234, date de naissance).
- Je garde secrets mes codes et identifiants professionnels

b2 **Gérer les pièces jointes et liens avec prudence**

- Ne cliquez pas sur des liens inconnus ou des pièces jointes suspectes, même par SMS ou messagerie instantanée.
- Méfiez-vous du phishing.

b3 **Je ne clique ni ne scanne sans vérifier la source**

- Réduction significative du risque d'infection par des malwares ou virus.
- Réduction des chances d'être victime de phishing ou de fraude en ligne.

b5 **Attention aux connexions réseau**

- Évitez les Wi-Fi publics non sécurisés (ex. : cafés, aéroports).
- Utilisez un VPN fourni par votre entreprise si possible.

Je désactive le Wi-Fi et le Bluetooth lorsque je ne les utilise pas.

b6 **Installer uniquement les applications nécessaires**

- Téléchargez les apps depuis des sources officielles (Google Play, App Store).
- Évitez les applications non professionnelles ou douteuses.
- Je demande toujours l'accord de mon service informatique avant d'installer quoi que ce soit

c'

c1 - Je n'utilise mon téléphone intelligent professionnel que pour des activités professionnelles.
- Je ne prête jamais mon téléphone intelligent professionnel, même pour dépanner, ou se divertir
- Je n'apporte pas mon téléphone professionnel en vacances avec moi.

c2 - Je m'assure que mes câbles et chargeurs sont fiables et certifiés.
- Je me tiens à l'écart des ports de recharge publics.

c3 - Je fais attention aux signes de comportement anormal de mon smartphone.
- Signaler immédiatement toute activité suspecte (applications qui plantent, messages inconnus, surchauffe inhabituelle).

Quand il y a un doute ; il y a un doute ! Prévenait toujours votre service informatique dans ce cas.

Pour toutes questions ou suggestions d’amélioration.

Michel Panouillot - contact@ubik-infosec.ca - ubik-infosec.ca

A propos de l’auteur

Professionnel chevronné en sécurité de l'information, je cumule plus de dix ans d’expérience dans des environnements complexes et diversifiés, incluant les secteurs gouvernementaux, de la formation et militaire. Mon expertise est centrée

sur l’analyse en cybersécurité, avec une spécialisation en gouvernance et conformité réglementaire.