

5 conseils pour sécuriser l'utilisation des téléphones mobiles au sein de votre entreprise

INFOGRAPHIE

Utiliser vos smartphones en toute sécurité

La sécurité informatique et la protection des données sont les préoccupations principales de Synovo Group et concernent tous les professionnels, quel que soit leur secteur d'activité. Vos équipes utilisent certainement régulièrement des téléphones portables équipés d'applications et / ou d'outils nécessaires à votre activité.

Nous vous partageons aujourd'hui 5 conseils et bonnes pratiques à mettre en place afin de sécuriser l'utilisation quotidienne de vos téléphones.





Inciter la mise en place d'une authentification



Utiliser un bloqueur d'applications



Etablir des procédures en cas de perte ou vol







une politique de MDM*

*Mobile Device Management

Inciter la mise en place d'**une authentification** sur les téléphones

POURQUOI EST-CE IMPORTANT?

L'authentification sur un téléphone mobile renforce la sécurité en s'assurant que seuls les utilisateurs autorisés peuvent accéder aux données et aux fonctionnalités de l'appareil, protégeant ainsi la vie privée et les informations sensibles. De plus, elle permet de prévenir le vol ou l'utilisation non autorisée de l'appareil, renforçant ainsi la protection de l'utilisateur.



d'applications

Utiliser un **bloqueur**



Un bloqueur d'applications sur un téléphone mobile permet de limiter, voire bloquer totalement, l'accès à certaines applications.

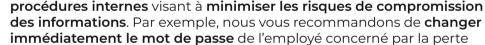
A QUOI SERT UN BLOQUEUR D'APPLICATIONS ?

Des solutions gratuites ou payantes existent pour vous aider à autoriser uniquement les applications nécessaires à votre activité.

Etablir des procédures

en cas de perte ou de vol

POURQUOI EST-CE IMPORTANT ?



ou le vol de son *smartphone*.

Les pertes ou vols peuvent survenir à tout moment. Afin de faire face à

de telles situations, il est essentiel d'établir dès maintenant des



POURQUOI EST-CE IMPORTANT ? La sensibilisation des employés à la sécurité des téléphones mobiles contribue à réduire les risques de vols et de cyberattaques, renforçant ainsi la sécurité de l'entreprise. Elle encourage également de bonnes

Sensibiliser vos employés à la cybersécurité



pratiques en matière de protection des informations confidentielles

(exemple : éviter d'écrire son mot de passe sur un post-it).

Le Mobile Device Management, ou gestion des terminaux mobiles en français, est un domaine d'administration qui gère le déploiement, la sécurisation, la surveillance, l'intégration et l'administration des appareils mobiles (smartphones, tablettes, ordinateurs) sur le lieu de travail. Une politique de MDM permet par exemple aux administrateurs

Faciliter la distribution de

politiques de sécurité,

augmentant ainsi

l'efficacité opérationnelle

CONTACT

Mettre en place une politique de

Mobile Device Management (MDM)

QUELS SONT LES AVANTAGES ?

La mise en place d'une solution de MDM offre divers avantages. Elle permet notamment de :

de contrôler les fonctionnalités au niveau des appareils (désactivation

d'applications, accès restreint à certaines fonctions, etc.).

accrue sur l'utilisation

des appareils, **optimisant**

la prise de décision et

réduisant les coûts liés à la

gestion des smartphones

Centraliser et sécuriser
la gestion des appareils
mobiles de ses employés,
améliorant ainsi la sécurité

des données

Qu'est-ce qu'une politique de mdm ?

Vous souhaitez en savoir plus ?

Pour toute demande d'informations et / ou d'accompagnement dans la mise en place d'une politique de MDM, notre équipe se tient à votre disposition.

RCS Strasbourg: 790 710 735

8 Rue Schertz 67100 STRASBOURG