INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

APPAREILS MOBILES
10 bonnes pratiques !

Les appareils mobiles "intelligents" contiennent des informations sensibles.
Ils sont plus faciles à perdre ou à se faire voler qu'un ordinateur.
Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

1 METTEZ EN PLACE ET COMPLEXIFIEZ LES CODES D'ACCÈS

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires empêcheront une personne malintentionnée de prendre le contrôle de votre appareil en cas de perte ou de vol et donc d'accéder à vos informations. Évitez les codes 1234 ou 0000.

CHIFFREZ LES DONNÉES DE L'APPAREIL 2

Le chiffrement des données vous assurera la non intrusion d'une personne malintentionnée. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ

Installez les mises à jour car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

FAÎTES DES SAUVEGARDES 4

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement, car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS 6

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications installées ne sont pas piégées. Privilégiez App Store pour IOS et Playstore pour Android.

7 CONTRÔLEZ LES AUTORISATIONS DE VOS APPLICATIONS

Vérifiez les autorisations que vous donnez à vos applications lors de leur installation (géolocalisation, accès à vos contacts ou à vos photos), mais aussi après des mises à jour car les autorisations peuvent évoluer. Vous pouvez à tout moment modifier ces autorisations depuis vos paramètres.

NE LAISSEZ PAS VOTRE APPAREIL SANS SURVEILLANCE 8

Il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU PARTAGÉS

L'accès à ces réseaux, même protégé par un mot de passe, peut être contrôlé par des cybercriminels qui peuvent intercepter vos connexions et récupérer vos données confidentielles.
Privilégiez une connexion cellulaire de type 3/4/5G.

NE STOCKEZ PAS D'INFORMATIONS CONFIDENTIELLES SANS PROTECTION 10

Ne notez jamais d'informations secrètes dans un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer.

inforsud-technologies.com 0 811 349 609

« Cybermalveillance.gouv.fr – Données originales téléchargées sur Cybermalveillance.gouv.fr, publié le 11/2019. »