SENSIBILISATION AUX RISQUES NUMÉRIQUES 3

Recommandations de Cybermalveillance.gouv.fr

	Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles.

1. METTEZ EN PLACE LES CODES D'ACCÈS

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires (voir encadré) empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

CODE D'ACCÈS
ET CODE PIN,
DEUX PROTECTIONS COMPLÉMENTAIRES

Mot de passe, signe, combinaison de touches ou biométrie : **le code de verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas.**

Composé de 4 chiffres, **le code PIN bloque quant à lui l'accès à votre carte SIM** et empêche donc de pouvoir s'en servir dans un autre appareil si on ne le connaît pas.

2. CHIFFREZ LES DONNÉES DE L'APPAREIL

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3. APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ

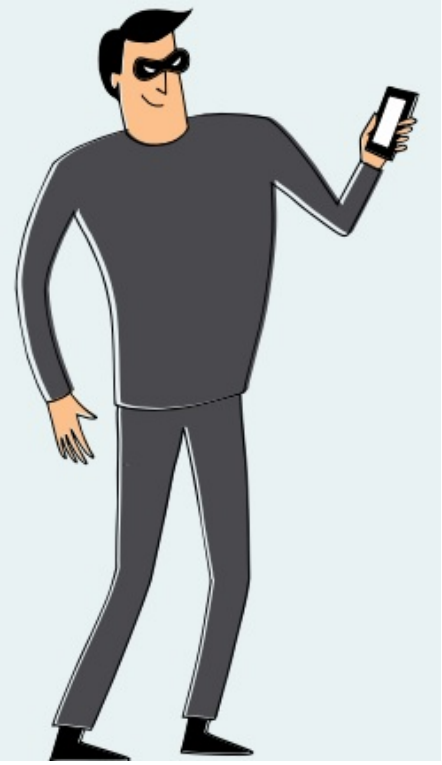
Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4. FAITES DES SAUVEGARDES

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 que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (ransomware), l'hameçonnage (phishing)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

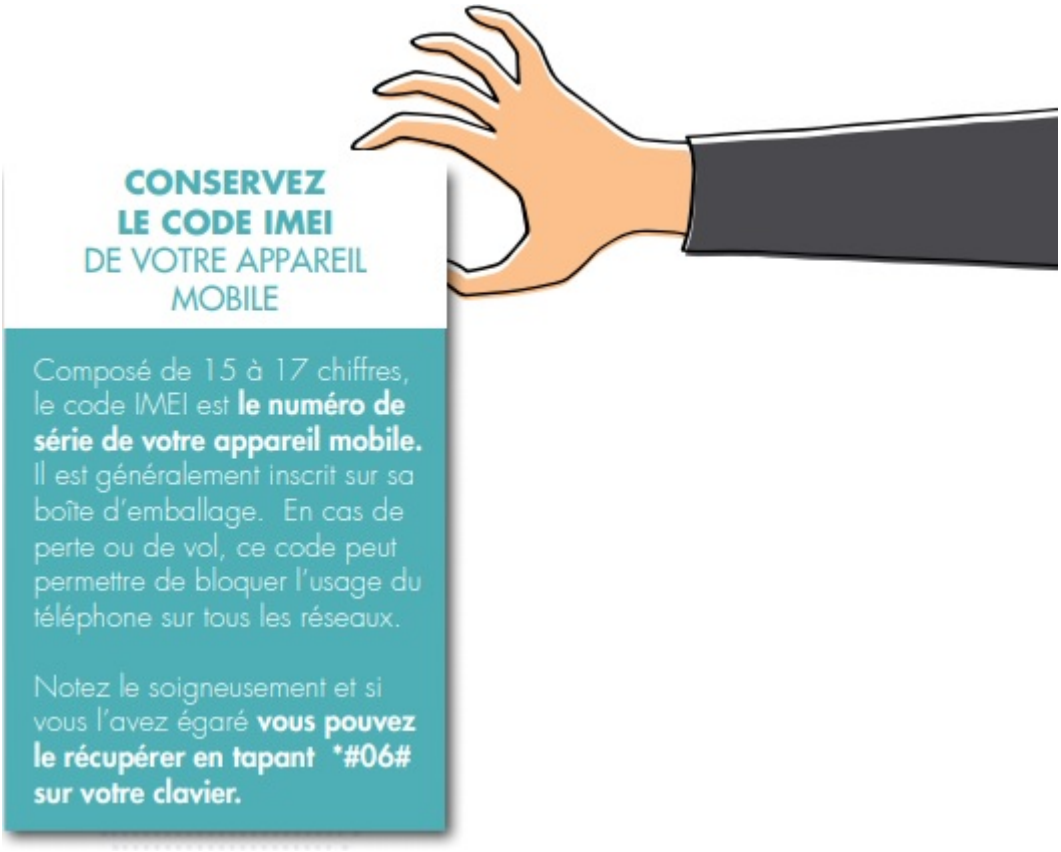


6. N’INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu’ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d’installer une nouvelle application. Au moindre doute, n’installez pas l’application et choisissez-en une autre

7. CONTRÔLEZ LES AUTORISATIONS DE VOS APPLICATIONS

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l’autorisation d’accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n’installez pas l’application et choisissez-en une autre.



8. NE LAISSEZ PAS VOTRE APPAREIL SANS SURVEILLANCE

Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9. ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

10. NE STOCKEZ PAS D'INFORMATIONS CONFIDENTIELLES SANS PROTECTION

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

RÉSUMÉ

10 CONSEILS POUR SÉCURISER VOTRE APPAREIL MOBILE
1 Mettez en place les codes d'accès
2 Chiffrez les données de l'appareil
3 Appliquez les mises à jour de sécurité
4 Faites des sauvegardes
5 Utilisez une solution de sécurité contre les virus et autres attaques
6 N'installez des applications que depuis les sites ou magasins officiels
7 Contrôlez les autorisations de vos applications
8 Ne laissez pas votre appareil sans surveillance
9 Évitez les réseaux Wi-Fi publics ou inconnus
10 Ne stockez pas d'informations confidentielles sans protection