

# Votre appareil mobile est-il sécurisé ?

Nous avons pratiquement tous un smartphone, mais combien d'entre nous pensent réellement aux menaces de sécurité auxquelles sont confrontés nos appareils mobiles ? Les appareils mobiles sont exposés à de nombreux types de menaces. Le nombre d'attaques visant les appareils mobiles est en augmentation, et des applications malveillantes les ciblent spécifiquement. Les cybercriminels peuvent ainsi voler des informations professionnelles comme personnelles à votre insu.

Même si vous avez installé une application antivirus ou de sécurité, cela ne suffit pas à sécuriser votre smartphone. La meilleure stratégie de défense contre les problèmes de confidentialité et de sécurité sur votre appareil mobile consiste à améliorer vos pratiques de sécurité mobile.

## Comment améliorer mes pratiques de sécurité mobile ?

N'oubliez jamais ces pratiques exemplaires pour limiter les risques d'instrumentalisation de vos appareils mobiles :

1. **Assurez-vous que le système d'exploitation de votre téléphone est toujours à jour.** Les systèmes d'exploitation sont souvent mis à jour pour corriger des failles de sécurité. De nombreuses attaques exploitent des failles de sécurité non corrigées sur les systèmes d'exploitation qui n'ont pas été mis à jour.
2. **Faites attention aux applications malveillantes dans votre magasin d'applications.** Les magasins d'applications officiels suppriment les applications contenant des programmes malveillants, mais il arrive que certaines d'entre elles passent entre les mailles du filet et puissent être téléchargées par des utilisateurs peu méfiants. Faites des recherches, lisez les évaluations et soyez attentif au nombre de téléchargements d'une application. Ne téléchargez jamais une application ailleurs que dans les magasins d'app officiels.
3. **Assurez-vous que les applications ne demandent pas accès à des éléments de votre téléphone qui ne sont pas pertinents pour la fonction qu'elles remplissent.** Les applications demandent ordinairement l'autorisation d'accéder à des fichiers, à des dossiers, à d'autres applications et à des données avant de les télécharger. N'accordez pas aveuglément ces autorisations. Si une demande d'autorisation ne vous semble pas justifiée, cherchez une autre application dans votre magasin d'apps.
4. **Pas de mot de passe ou une protection par mot de passe insuffisante.** De nombreuses personnes n'utilisent toujours pas de mot de passe pour verrouiller leur téléphone. Si votre appareil est perdu ou volé, le voleur aura facilement accès à toutes les informations stockées sur votre téléphone.
5. **Méfiez-vous du Wi-Fi public. Les cybercriminels exploitent la technologie pour voir ce que vous faites.** Évitez de vous connecter à des services en ligne ou d'effectuer des opérations sensibles (comme des transactions bancaires) sur du Wi-Fi public.



L'équipe de sécurité KnowBe4