

À quel point votre appareil mobile est-il sécurisé?

La plupart d'entre nous possèdent un téléphone intelligent, mais combien parmi nous s'interrogent sur les menaces de sécurité auxquelles nous sommes exposés à cause de ces appareils mobiles? Les appareils mobiles sont vulnérables à différents types de menaces. Les pirates intensifient leurs attaques sur les appareils mobiles et ciblent votre téléphone par le biais d'applications malveillantes. Grâce à ces méthodes, ils peuvent voler des informations personnelles et professionnelles sans que vous vous rendiez compte de ce qui se passe.

Même si vous avez téléchargé une application de sécurité ou un antivirus, la protection de votre téléphone intelligent va au-delà de ces services. Votre meilleure défense contre les problèmes de confidentialité et de sécurité liés à votre appareil mobile est d'améliorer vos pratiques de sécurité mobile.

Comment puis-je améliorer mes pratiques de sécurité mobile?

Souvenez-vous toujours des pratiques exemplaires suivantes pour minimiser les risques d'exploits sur vos appareils mobiles :

- 1. Assurez-vous que le système d'exploitation de votre téléphone est systématiquement à jour.** Les systèmes d'exploitation sont souvent mis à jour de manière à corriger des failles de sécurité. Plusieurs menaces proviennent d'un système d'exploitation obsolète, dans lequel les failles de sécurité n'ont pas été corrigées.
- 2. Méfiez-vous des applications malveillantes qui se trouvent dans les boutiques d'applications.** Les boutiques d'applications officielles suppriment régulièrement des applications contenant des maliciels, mais parfois, certaines de ces dangereuses applications passent à travers les mailles du filet et peuvent donc être téléchargées par des utilisateurs non avertis. Faites des recherches, lisez les commentaires et portez attention au nombre de téléchargements. Ne téléchargez jamais d'applications à partir d'autres sources que les boutiques d'applications officielles.
- 3. Assurez-vous que les applications ne vous demandent pas d'accéder à des éléments de votre téléphone qui n'ont rien à voir avec leur fonction.** Avant leur téléchargement, les applications demandent habituellement toute une liste d'autorisations pour accéder à des fichiers, à des dossiers, à d'autres applications et à des données. N'accordez pas aveuglément toutes les autorisations demandées. Si les demandes d'autorisations ne vous semblent pas pertinentes, recherchez une alternative dans votre boutique d'applications.
- 4. Aucun mot de passe ou une protection par mot de passe faible.** De nombreuses personnes n'utilisent toujours pas de mot de passe pour verrouiller leur téléphone. Si votre appareil est perdu ou volé, les voleurs accéderont facilement à l'ensemble des informations stockées sur votre téléphone.
- 5. Soyez prudent lorsque vous utilisez les réseaux WiFi publics.** Les technologies dont se servent les escrocs leur permettent de voir ce que vous faites. Évitez de vous connecter à vos services en ligne ou d'effectuer des transactions sensibles, comme des opérations bancaires, lorsque vous utilisez un réseau WiFi public.



L'équipe de sécurité KnowBe4