Comment aider à sécuriser vos appareils mobiles

Par Patrick Sentinel – 29a.ca

Les smartphones et tablettes sont devenus des extensions de nos vies, contenant une quantité impressionnante d'informations personnelles et professionnelles. Avec l'augmentation des menaces numériques, il est important de rendre ces appareils plus sécuritaires pour protéger vos données personnelles et sensibles. Cet article vous guidera à travers les étapes essentielles pour renforcer la sécurité de vos appareils mobiles.

1. Activer le verrouillage de l'écran

Le verrouillage de l'écran est la première barrière de sécurité pour votre appareil mobile. Il aide à empêcher quiconque d'accéder à votre téléphone sans votre permission.

- **Utilisez un code PIN ou un mot de passe fort** : Optez pour un code PIN d'au moins 6 chiffres ou un mot de passe comprenant des lettres, des chiffres, et des symboles.
- **Activez la reconnaissance biométrique** : La reconnaissance faciale ou l'empreinte digitale sont des options rapides pour déverrouiller votre appareil. **Cependant, certains appareils mobiles ont été déverrouillés à l'aide de photos ou d'images biométriques du visage du propriétaire.**
- **Configurer le verrouillage automatique** : Réglez votre appareil pour qu'il se verrouille automatiquement après une période d'inactivité, idéalement après 30 secondes.

2. Mettre à jour le système et les applications

Les mises à jour régulières sont essentielles pour corriger les vulnérabilités de sécurité découvertes dans votre système d'exploitation et vos applications.

- **Activez les mises à jour automatiques** : Assurez-vous que votre appareil est configuré pour télécharger et installer automatiquement les mises à jour dès qu'elles sont disponibles.
- **Vérifiez manuellement les mises à jour** : parfois, certaines mises à jour nécessitent une confirmation manuelle. Prenez l'habitude de vérifier régulièrement si des mises à jour sont disponibles pour votre système d'exploitation et vos applications.
- **Supprimez les applications obsolètes** : Si vous avez des applications que vous n'utilisez plus ou qui ne sont plus mises à jour, désinstallez-les pour diminuer les risques de sécurité. *** Ce point est trop souvent sous-estimé *** Vous n'utilisez pas une application alors supprimez là!

3. Télécharger des applications de sources fiables

Les applications peuvent être une porte d'entrée pour les logiciels malveillants. Téléchargez-les uniquement à partir de sources fiables pour éviter d'infecter votre appareil.

- **Utilisez les magasins officiels** : Téléchargez vos applications uniquement depuis le *Google Play Store* ou *l'App Store d'Apple*. Évitez les sites tiers qui proposent des applications non vérifiées.
- **Lisez les avis et vérifiez les permissions** : Avant d'installer une application, lisez les avis des utilisateurs et vérifiez les permissions qu'elle demande. Une application qui demande des accès excessifs ou à trop de fonctionnalités (comme vos contacts ou votre appareil photo) peut être suspecte.
- **Méfiez-vous des applications trop généreuses** : Si une application gratuite promet des fonctionnalités premium ou trop belle pour être vraies, soyez prudent. Ces applications peuvent cacher des intentions malveillantes.

4. Protéger vos données avec le chiffrement

Le chiffrement est une mesure de sécurité avancée qui protège vos données en les rendant illisibles pour toute personne non autorisée.

- **Activez le chiffrement sur votre appareil** : La plupart des smartphones modernes offrent une option de chiffrement des données. Assurez-vous que cette fonctionnalité est activée dans les paramètres de sécurité de votre appareil. Parfois, le chiffrement est activé par défaut!
- **Chiffrez vos sauvegardes** : Si vous enregistrez vos données sur un ordinateur ou dans le nuage, assurez-vous que ces sauvegardes sont également chiffrées. Cela empêche l'accès non autorisé à vos informations en cas de vol ou de piratage.
- **Utilisez des applications de messagerie chiffrée** : Préférez les applications qui offrent le chiffrement de bout en bout, comme *Signal* ou *WhatsApp*, pour aider à protéger vos communications.

5. Être prudent avec les réseaux Wi-Fi publics (un MUST)

Les réseaux Wi-Fi publics sont pratiques, mais **ils peuvent être très dangereux** si vous n'adoptez pas les bonnes pratiques de sécurité.

- **Évitez les transactions sensibles** : Ne faites pas d'achats en ligne, n'accédez **SURTOUT PAS** à vos comptes bancaires, ou n'envoyez pas d'informations personnelles sensibles **lorsque vous êtes connecté à un réseau Wi-Fi public**.
- **Utilisez un VPN** : Un réseau privé virtuel (VPN) chiffre votre connexion Internet, rendant vos activités en ligne plus sécurisées, même sur des réseaux publics.
- **Désactivez le Wi-Fi et le Bluetooth lorsque vous ne les utilisez pas** : Cela empêche votre appareil de se connecter automatiquement à des réseaux ou appareils non sécurisés à proximité.

6. Sauvegarder régulièrement vos données

Les sauvegardes régulières sont essentielles pour récupérer vos informations en cas de perte, de vol, ou de panne de votre appareil.

- **Utilisez le nuage** : Activez les sauvegardes automatiques vers des services de nuage sécurisés comme *Google Drive* ou *iCloud*. Cela aide à récupérer vos données si vous perdez votre appareil. Cependant, attention aux informations que vous y déposez! Ne déposez pas d'informations sensibles à moins qu'elles soient chiffrées avec un algorithme reconnu par l'industrie.
- **Faites des copies locales** : En plus du nuage, envisagez de faire des sauvegardes locales sur un disque dur externe ou un ordinateur. Cela offre une couche supplémentaire de protection.
- **Vérifiez vos sauvegardes** : Assurez-vous que vos sauvegardes se font correctement et que toutes les données importantes sont incluses.

Conclusion

La sécurité de vos appareils mobiles ne doit pas être négligée. En suivant ces étapes simples, vous pouvez considérablement réduire les risques de perdre vos données ou de devenir victime de cybercriminalité. Prenez le temps de configurer correctement la sécurité de vos appareils et restez vigilant face aux nouvelles menaces.