

OUCH!

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

# Sécuriser vos appareils mobiles

## Vue d'ensemble

Vos appareils mobiles constituent un moyen simple et étonnant de communiquer avec vos amis, de faire des achats en ligne ou de faire des transactions bancaires en ligne, de regarder des films, de jouer à des jeux et d'effectuer une myriade d'autres activités. Étant donné que vos appareils sont une partie importante de votre vie, voici quelques étapes simples pour assurer votre sécurité et celle de vos appareils.

## Sécuriser vos appareils

Cela peut vous surprendre de savoir que le plus grand risque pour votre appareil mobile n'est pas le piratage, mais probablement vous. Vous êtes en effet beaucoup plus susceptible de perdre ou d'oublier votre appareil mobile que de vous le faire pirater. La première chose que vous devriez faire pour protéger vos appareils est de permettre le verrouillage automatique de l'écran, souvent appelé un verrouillage d'écran. Cela signifie que chaque fois que vous voulez utiliser votre appareil, vous devez d'abord déverrouiller l'écran, par exemple avec un mot de passe fort ou votre empreinte digitale. Cela permet de s'assurer que si votre appareil est perdu ou volé, personne ne peut y accéder. En outre, voici plusieurs autres conseils pour vous aider à protéger vos appareils:

### ✓ Mise à jour

activez la mise à jour automatique sur vos appareils afin qu'ils exécutent toujours la dernière version du système d'exploitation et des applications. Les attaquants sont toujours à la recherche de nouvelles faiblesses dans les logiciels, et les fournisseurs publient constamment de nouvelles mises à jour et correctifs pour les corriger. En utilisant toujours le dernier système d'exploitation et les dernières applications mobiles, il est beaucoup plus difficile pour quiconque de pirater vos appareils.

### 📍 Suivi

installez ou activez le logiciel pour suivre à distance votre appareil mobile sur Internet. De cette façon, si votre appareil est perdu ou volé, vous pouvez vous connecter sur Internet et trouver son emplacement ou, dans le pire des cas, effacer à distance toutes vos informations.

### ✓ Applications approuvées

téléchargez uniquement les applications dont vous avez besoin et provenant de sources fiables. Pour les iPads ou les iPhones, cela signifie télécharger des applications depuis l'Apple App Store. Pour Android télécharger des applications

à partir de Google Play et pour les tablettes Amazon sur l'Amazon App Store. Bien que vous puissiez télécharger des applications à partir d'autres sites, ceux-ci ne sont pas vérifiés et sont beaucoup plus susceptibles d'être infectés. En outre, avant de télécharger une application, vérifiez qu'elle contient de nombreux avis positifs et qu'elle est mise à jour activement par le fournisseur. Restez à l'écart des toutes nouvelles applications, applications avec peu de critiques ou rarement mises à jour. Enfin, quel que soit l'endroit où vous avez reçu votre application, une fois que vous n'en avez plus besoin ou que vous ne l'utilisez plus, nous vous recommandons de la supprimer de votre appareil.

## Options de confidentialité

Lors de l'installation d'une nouvelle application, assurez-vous de revoir les options de confidentialité. Par exemple, l'application que vous venez de télécharger doit-elle vraiment avoir accès à toutes vos informations d'amis et de contacts? Nous vous recommandons également de désactiver le suivi de l'emplacement pour tout, puis d'activer l'emplacement pour les applications dont vous pensez avoir besoin. Si vous n'êtes pas à l'aise avec les exigences d'autorisation d'une application, trouvez-en une autre qui réponde à vos besoins. En outre, vérifiez régulièrement les autorisations pour vous assurer qu'elles n'ont pas été modifiées.

## Sauvegardes

Toujours sauvegarder vos données. Pour les appareils mobiles, une grande partie de vos informations est souvent sauvegardée automatiquement, comme vos photos ou vos messages. Toutefois, les sauvegardes stockent également votre configuration, vos applications et d'autres informations sur les périphériques, ce qui facilite grandement la récupération à partir d'un périphérique perdu ou la transition vers un nouveau périphérique.

## Travail

Lorsque vous êtes au travail, faites très attention et ne prenez jamais de photos ou de vidéos qui pourraient contenir accidentellement des informations sensibles, comme des photos de tableaux blancs ou d'écrans d'ordinateur.

Vos appareils mobiles sont un outil puissant, que nous voulons que vous appréciez et utilisiez. Il suffit de suivre ces quelques étapes simples afin de pouvoir garder vos périphériques sécurisés.

## Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

## Sources

Phrases de passe :	<a href="https://www.sans.org/u/A3E">https://www.sans.org/u/A3E</a>
Sauvegarde/Restauration :	<a href="https://www.sans.org/u/A3z">https://www.sans.org/u/A3z</a>
Mise au rebut de votre appareil mobile :	<a href="https://www.sans.org/u/A3u">https://www.sans.org/u/A3u</a>
Utilisation sécurisée des applications mobiles :	<a href="https://www.sans.org/u/A3p">https://www.sans.org/u/A3p</a>
Astuce de sécurité SANS du jour :	<a href="https://www.sans.org/tip_of_the_day.php">https://www.sans.org/tip_of_the_day.php</a>

## Licence

OUCH! est publiée par le programme SANS « sécuriser l'humain » (Securing The Human) et est distribuée sous la licence « [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subie aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet