

OUCH!

Dans ce numéro...

- Sécuriser votre tablette
- Garder votre tablette sécurisée

Sécuriser votre nouvelle tablette

Vue d'ensemble

Félicitations pour l'acquisition de votre nouvelle tablette ! Cette technologie est un moyen puissant et pratique pour communiquer avec autrui, pour faire des achats en ligne, regarder des films, jouer à des jeux et effectuer une multitude d'autres activités. Etant donné que ce nouvel outil peut prendre une place importante dans votre vie quotidienne, peut-être même remplacer votre ordinateur, voici quelques étapes clés que vous pouvez prendre en considération pour maintenir votre tablette ainsi que vos informations sûres et sécurisées.

Editeur invité

Lori Rosenberg possède une vaste expérience dans le développement de la sécurité informatique de matériel éducatif et de formation pour les employés et clients, et se passionne également pour trouver des méthodes nouvelles et intéressantes pour partager cette connaissance. Vous pouvez la trouver sur Twitter à [InfoSecLori](#).

Sécuriser votre tablette

Cela pourra vous paraître surprenant mais sachez que le plus grand risque qu'encourt votre tablette ne sont pas des pirates, le plus probable est que ça soit vous. Vous êtes en effet beaucoup plus susceptible de perdre, oublier ou de vous faire voler votre tablette et d'avoir ainsi quelqu'un qui la pirate. La première chose que vous devez faire pour protéger votre tablette est d'activer le verrouillage automatique de l'écran. Cela signifie qu'à chaque fois que vous voulez utiliser votre tablette, vous devez d'abord déverrouiller l'écran avec un mot de passe fort, utiliser un schéma de déverrouillage ou encore votre empreinte digitale. Cela vous garantit que si votre tablette est perdue ou volée, personne ne pourra accéder à l'ensemble de vos informations personnelles et à vos applications mobiles. Une fois que le verrouillage automatique de l'écran est activé, voici quelques conseils supplémentaires qui vous aideront à protéger efficacement votre nouvelle tablette:

- Installez ou activez un logiciel pour suivre à distance votre nouvelle tablette au travers d'Internet. De cette façon, si votre tablette est perdue ou volée, vous pouvez potentiellement vous y connecter depuis Internet et définir son emplacement, ou dans le pire des cas, effacer à distance toutes vos informations qu'elle contient.
- Mettez à jour votre appareil et activez la mise à jour automatique de manière à exécuter toujours la dernière version du système d'exploitation. Les attaquants sont toujours à la recherche de nouvelles failles du logiciel, et les vendeurs sont constamment en train de publier de nouveaux correctifs et des mises à jour pour les corriger. En exécutant toujours le dernier système d'exploitation et la dernière version de vos applications mobiles, vous rendez ainsi beaucoup plus difficile pour quiconque de pirater votre tablette.

Sécuriser votre nouvelle tablette

- Faites attention lorsque vous configurez votre tablette pour la première fois, en particulier lors de la mise en place des options de confidentialité. Un des problèmes majeurs relatif à la vie privée est la possibilité pour autrui de suivre et de connaître votre emplacement. Nous vous recommandons de désactiver le suivi de localisation pour tout, activer uniquement la géolocalisation pour les applications pour lesquelles vous en ressentez le besoin. Pour certaines applications, il est important d'être en mesure de suivre votre position, comme par exemple un logiciel de cartographie ou encore pour trouver un restaurant local, mais la plupart de vos applications n'ont pas besoin d'informations de localisation en temps réel.
- La plupart des tablettes et applications stockent vos informations dans le Cloud. En tant que tel, assurez-vous de bien comprendre où vos données se trouvent et comment elles sont sécurisées. Par exemple, la dernière chose que vous voulez est que vos photos privées soient partagées sur Internet et que le monde entier puisse les voir, avec des informations de géolocalisation intégrées. Par défaut, désactivez tout partage de toute information dans le Cloud, autorisez-lui seulement quand vous voulez partager quelque chose de spécifique.
- Les tablettes synchronisent de plus en plus vos applications avec d'autres dispositifs tels que votre smartphone ou votre ordinateur portable. La synchronisation peut être une caractéristique formidable, mais attention aux applications ou fonctionnalités que vous autorisez à synchroniser. Si vous avez activé la synchronisation, ne soyez pas surpris de voir les sites que vous avez visités et les onglets que vous avez créés sur le navigateur de votre tablette.



La meilleure façon de vous assurer que votre tablette est sécurisée est de permettre le verrouillage d'écran, vérifier les paramètres de confidentialité et de garder votre tablette à jour.

Garder votre tablette sécurisée

Une fois que vous avez sécurisé votre tablette, vous voulez être sûr qu'elle le reste. Voici quelques étapes clés à prendre en considération pour que votre tablette reste sécurisée à long terme.

- Ne jamais jailbreaker ou pirater votre propre tablette. Cela permettra de contourner et de rendre inutile un très grand nombre de contrôles de sécurité et de rendre ainsi votre tablette beaucoup plus vulnérable aux attaques.
- Télécharger uniquement les applications dont vous avez besoin et à partir de sources de confiance. Pour les iPads, télécharger uniquement des applications à partir d'iTunes. Ces applications sont examinées par Apple avant qu'elles ne soient mises à disposition. Concernant Google, nous vous recommandons de télécharger des applications depuis

Sécuriser votre nouvelle tablette

Google Play et seulement pour la tablette d'Amazon, nous vous recommandons de rester sur l'Amazon App Store. Il est clair que vous pouvez télécharger des applications à partir d'autres sites, cependant, ceux-ci ne sont pas contrôlés et pourraient être infectés. Enfin, peu importe où vous avez obtenu votre application, une fois que vous ne l'utilisez plus activement, nous vous conseillons de la supprimer de votre tablette.

- Lorsque vous installez une nouvelle application, assurez-vous d'examiner et de définir les options de confidentialité, tout comme vous l'avez fait lors de la configuration initiale de votre nouvelle tablette. Faites bien attention aux informations auxquelles vous autorisez l'accès ainsi que ce que vous laissez faire par vos différentes applications de ces mêmes informations. Par exemple, est-ce l'application que vous venez de télécharger a vraiment besoin d'accéder à tous vos contacts ? 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 afin de vous assurer qu'elles n'ont pas changées.

Votre tablette est un outil puissant, un de ceux que vous aimez et utilisez. Rappelez-vous que les quelques étapes simples susmentionnées peuvent vous permettre de garder votre tablette sécurisée un long moment.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants :

<http://www.answer.ch> et <http://answersecurity.com/>

Sources

Utiliser les appareils mobiles de manière sécurisée : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_fr.pdf

Phrases de passe : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_fr.pdf

Utilisation du Cloud en toute sécurité : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201409_fr.pdf

Mise au rebut de votre équipement mobile : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201406_fr.pdf

Conseil du jour de l'institut SANS : https://www.sans.org/tip_of_the_day.php

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 ouch@securingthehuman.org.

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner

Traduit par : Marilyn Combet



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.org/gplus