OUCH! | Décembre 2016

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

OUCH!

Dans ce numéro...

Comment se séparer de votre appareil mobile de façon sécurisée ?

Vue d'ensemble

Les appareils mobiles comme les smartphones, les tablettes ou encore les montres connectées continuent d'évoluer et d'innover à un rythme extrêmement rapide. Certaines personnes changent même leurs smartphones tous les ans. Malheureusement beaucoup trop d'individus se débarrassent de leurs appareils sans penser à toutes les informations personnelles que ceux-ci peuvent contenir. Dans cette newsletter, nous allons voir quelles sont les informations qui sont stockées sur votre appareil ainsi que la façon dont vous pouvez les effacer de manière sécurisée avant de vous en débarrasser. Si vous avez un appareil mobile fourni par votre employeur, ou bien si vous avez des informations organisationnelles stockées dessus, assurez-vous auprès de votre employeur que tous les backups nécessaires ont été réalisés avant de suivre les conseils que nous vous fournissons.

Editeur invité

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) est l'analyste forensic principale au sein de ManTech CARD. Elle a participé à la création de cours au sein du SANS Institute, notamment sur l'Analyse Forensic avancée des smartphones. Elle est également instructrice pour le cours d'analyse forensic Windows. Elle participe au blog **smarterforensics.com**.

Vos Informations

Les appareils mobiles sont beaucoup plus sensibles que ce qu'il n'y parait, souvent même plus sensibles que votre ordinateur. Vous retrouverez en général les informations suivantes :

- Votre adresse, lieu de travail, les lieux que vous fréquentez
- Les coordonnées de tous vos contacts dans votre carnet d'adresse ou les applications. A savoir, votre famille, vos amis, vos collègues…
- L'historique de vos appels (entrants, sortants ou manqués)
- Les messages textes (SMS…), vocaux
- Les « chats » au sein d'applications de communication comme WhatsApp, les jeux ou les réseaux sociaux
- L'historique de vos déplacements basés sur vos coordonnées GPS ou antennes réseaux
- Votre historique de navigation web, vos recherches, les cookies de connections et les pages en cache
- Vos photos et vidéos personnelles, vos emails et les enregistrements vocaux
- Les mots de passe enregistrés et les accès aux comptes personnels tels que votre banque ou vos e-mails
- Vos informations personnelles stockées dans le Cloud
- Des informations de santé telles que votre âge, poids, pulsations cardiaques…

Comment se séparer de votre appareil mobile de façon sécurisée ?

Effacer votre appareil

Comme vous pouvez le constater, il y a possiblement une multitude d'informations sensibles sur vos appareils mobiles. Quelle que soit la façon dont vous allez vous débarrasser de votre appareil, si vous le donnez, si vous l'échangez pour un nouveau modèle, si vous le revendez ou même si vous le jetez, vous devez être certain d'avoir effacé toutes les informations sensibles. Vous ne le réalisez peut-être pas, mais si vos données sont simplement supprimées, elles peuvent être facilement récupérées grâce à des outils gratuits trouvés sur internet. Vous devez par conséquent effacer les données sur votre appareil de manière sécurisée. Vous pouvez écraser vos données afin d'empêcher toute action pour les récupérer ou en les rendant irrécupérables. Rappelez-vous, avant d'effacer vos données, vous devez effectuer une sauvegarde au préalable afin de les transférer facilement sur votre nouvel appareil.

Lorsque vous vous débarrassez de votre appareil mobile, vérifiez bien que vous avez fait un retour aux paramètres d'usine et que vous avez retiré la carte SIM ainsi que la carte mémoire.

La meilleure façon de procéder à l'effacement, c'est d'utiliser la fonction « retour aux paramètres d'usine ». Cela permettra de remettre votre appareil dans son état initial. Nous avons défini que le retour aux paramètres d'usine est le moyen le plus simple et le plus sécurisé de supprimer les données de votre appareil. Selon les marques, les fonctions de retour aux paramètres d'usine diffèrent. Vous trouverez ci-dessous les étapes vous permettant d'effectuer cet effacement pour les OS les plus fréquents.

- Appareils Apple iOS: Settings | General | Reset | Erase All Content and Settings
- Appareils Android: Settings | Privacy | Factory Data Reset

Malheureusement en ce qui concerne les appareils Windows, l'opération n'est pas aussi simple que de faire le retour aux paramètres d'usine. Des recherches sont encore en cours afin de déterminer la meilleure méthode avec les appareils Windows. Si vous avez de nouvelles questions concernant le retour aux paramètres d'usine, n'hésitez pas à regarder le site web du constructeur de votre appareil ou la notice d'exploitation de celui-ci. Rappelez-vous, simplement supprimer vos données n'est pas suffisant, car elles peuvent facilement être récupérées.

SIM et cartes mémoires

En plus de prendre en compte les données qui sont sur votre appareil, vous ne devez pas oublier de vous occuper de votre carte SIM (Subscriber Identity Module). La carte SIM est utilisée par l'appareil afin d'établir une connexion cellulaire (voix, données...). Le retour aux paramètres d'usine de votre téléphone n'impacte pas la carte SIM. Celle-ci stockera toujours des informations personnelles car elle est liée à l'utilisateur, vous. Si vous gardez votre numéro de téléphone, arrangez-vous

Comment se séparer de votre appareil mobile de façon sécurisée ?

pour pouvoir réutiliser la même carte SIM si celle-ci est compatible et que vous pouvez transférer votre abonnement. Si cela n'est pas possible car la taille de la carte SIM est différente, ou alors que votre nouvel opérateur ne peut pas réutiliser votre carte SIM, nous vous recommandons de garder votre carte pour la détruire physiquement. Pour ce faire vous pouvez la broyer ou alors la couper en morceau avec des ciseaux.

Certaines d'entre vous utilisez également une carte mémoire externe afin d'augmenter la capacité de stockage. Ces cartes mémoires contiennent la plupart du temps des photos, des applications ou d'autres informations sensibles. Pensez bien à la retirer lorsque vous vous débarrassez de votre appareil (Sur certains appareils la carte mémoire est cachée souvent derrière la batterie). Ces cartes peuvent être réutilisées sur d'autres appareils ou peuvent servir de support de stockage externe avec l'adaptateur adéquat. Si vous ne pouvez pas, ou ne souhaitez pas réutiliser votre carte, il faut la détruire de la même façon que votre carte SIM.

Si certains points abordés dans cette newsletter vous semblent nébuleux, apporter votre appareil dans le magasin ou vous l'avez acheté et demander de l'aide à un technicien. Pour finir, si vous envisagez de jeter votre appareil, n'hésitez pas à le donner à une œuvre caritative. Il y en a beaucoup qui sont intéressées par la récupération d'anciens appareils.

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

Protéger votre nouvelle tablette : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_fr.pdf

Sauvegarde et backup : https://securingthehuman.sans.org/ouch/2015#august2015

L'Analyse Forensic avancée des smartphones : https://sans.org/for585

Les archives de la Newsletter OUCH : https://securingthehuman.sans.org/ouch/archives

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley

Traduit par : Marilyn Combet