OUCH! | Juin 2014

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

OUCH!

Dans ce numéro...

- **Vos informations**
- **Formatage de votre équipement**
- **Cartes SIM et de stockage externes**

Mise au rebut de votre équipement mobile

Vue d'ensemble

Les appareils mobiles, tels que les smartphones et les tablettes, continuent de se développer et d'innover à un rythme étonnant. En conséquence, beaucoup d'entre nous remplaçons nos appareils mobiles le plus souvent tous les 18 mois. Malheureusement, trop de personnes se séparent simplement de leurs anciens équipements mobiles sans réellement tenir compte du volume de données personnelles que leurs appareils ont accumulé. Dans ce numéro, nous allons présenter les différents types de données personnelles pouvant être présentes sur votre équipement mobile ainsi que les manières de le formater en toute sécurité en vue de vous en séparer ou bien de le donner. Si votre équipement mobile vous a été attribué par votre employeur, ou bien s'il contient des données liées à votre entreprise, alors veillez à vérifier avec votre supérieur les procédures de sauvegarde et de mise au rebut adéquates avant de suivre les étapes ci-dessous.

Editeur invité

Christopher Crowley(**@CCrowMontance**;**+ChrisCrowley**) est un consultant basé dans l'Etat de Washington, DC. Il est instructeur en chef du cours Mobile Device Security and Ethical Hacking (SEC575) au SANS Institute et également auteur du cours Incident Response Team Management (MGT535).

Vos informations personnelles

Les équipements mobiles stockent bien plus de données sensibles que vous ne pouvez l'imaginer, probablement même plus que votre ordinateur. Les informations typiques stockées par ce type d'équipement peuvent inclure :

- L'endroit où vous vivez, où vous travaillez ainsi que les lieux où vous vous rendez habituellement ;
- Les coordonnées de l'ensemble de vos contacts présents dans votre carnet d'adresses, y compris de votre famille, de vos amis et de vos collègues ;
- L'historique de vos appels incluant les appels entrants, sortants et manqués ;
- Les messages textes et vocaux ;
- Les sessions de chat issues des applications telles que les jeux et les médias sociaux ;
- L'historique de géolocalisation basée sur les coordonnées GPS ou bien sur l'historique des émetteurs cellulaires ;
- L'historique de navigation Web, les cookies et les pages en cache ;
- Des photos personnelles, des vidéos, des enregistrements audio et des courriels ;
- Des mots de passe enregistrés et l'accès à des comptes personnels, tels que ceux pour votre banque en ligne ou service de messagerie ;
- L'accès à des photos, des fichiers ou des informations stockées dans le Cloud ;
- Toute information liée à votre santé, y compris votre rythme cardiaque, votre pression artérielle ou encore votre régime alimentaire.

Mise au rebut de votre équipement mobile

Formatage de votre équipement

Comme vous pouvez le voir, il peut y avoir une quantité impressionnante d'informations sensibles sur votre équipement mobile. Peu importe la manière dont vous vous séparez de votre équipement, que ce soit sous la forme d'un don, ou bien que vous le transmettiez à un autre membre de votre famille, que vous le revendiez ou même que vous le jetiez, vous devez en premier lieu être certain d'effacer toutes vos informations sensibles. En outre, vous devez également effacer vos informations si vous réinitialisez votre équipement ou bien l'échangez pour un nouveau. Si vous ne le faites pas, la personne qui reprendra votre équipement sera en mesure d'accéder facilement à vos informations sensibles. Toutefois, avant de commencer à effacer vos données, vous aurez probablement besoin de sauvegarder l'ensemble de celles-ci, incluant ainsi vos photos, vos vidéos ou toute autre information. Une fois le formatage de votre équipement terminé, vous ne serez plus en mesure de récupérer une quelconque donnée précédemment stockée sur ledit périphérique.

Lors de la mise au rebut de votre appareil mobile, assurez-vous d'effectuer une réinitialisation d'usine ainsi que de retirer la carte SIM et l'éventuelle carte SD si votre appareil en dispose.

Une fois que vous avez sauvegardé vos données, vous devez alors formater votre appareil en toute sécurité. Le fait de supprimer des fichiers, des photos ou des données n'est pas suffisant. En effet, les données qui ont été supprimées peuvent être facilement récupérées en utilisant des outils disponibles gratuitement sur Internet. Pour éviter cela, vous voulez effacer en toute sécurité l'ensemble des données présentes sur le périphérique : c'est ce que l'on appelle le formatage. Cela écrase les informations de sorte qu'elles ne puissent pas être récupérées. La façon la plus simple de le faire est d'utiliser la fonction "Réinitialisation aux paramètres d'usine" (Factory Reset). Il s'agira d'un retour à l'état initial lorsque vous l'avez acheté. Nous avons pu constater que la réinitialisation d'usine fournit la méthode la plus sûre et la plus simple pour effacer l'ensemble des données présentes sur votre équipement mobile. L'emplacement de la fonction de réinitialisation d'usine varie entre appareils ; ci-dessous la liste des étapes à suivre pour les trois équipements les plus populaires.

- Les périphériques Apple iOS : Réglages | Général | Réinitialiser | Effacer contenu et réglages.
- Les périphériques Android : Paramètres | Confidentialité | Réinitialiser les données d'usine.
- Les Windows Phones : Préférences | A propos | Réinitialiser votre téléphone.

Si vous avez encore des questions sur la façon d'effectuer une réinitialisation d'usine, consultez le manuel d'utilisation ou bien le site Web du constructeur. Rappelez-vous tout simplement que la suppression de vos données personnelles ne suffit pas car elles peuvent être facilement récupérées.

Cartes SIM et externes

Outre les données stockées sur votre équipement, vous devez également tenir compte de votre carte SIM (Subscriber Identity Module). Une carte SIM est l'élément sur lequel s'appuie un téléphone cellulaire ou encore une connexion de

Mise au rebut de votre équipement mobile

données. Lorsque vous effectuez une réinitialisation d'usine sur votre appareil, la carte SIM conserve des informations sur votre compte. Si vous souhaitez conserver votre numéro de téléphone et acheter à un nouvel appareil, parlez au vendeur du transfert de votre carte SIM. Si cela n'est pas possible, par exemple si votre nouveau téléphone utilise une taille de carte SIM différente, conservez votre ancienne carte SIM et déchiquetez-la physiquement ou détruisez-la pour empêcher quelqu'un d'autre de la réutiliser.

Enfin, certains équipements mobiles utilisent une carte SD séparée (Secure Digital) afin de fournir un stockage supplémentaire. Ces cartes de stockage contiennent souvent des images, des applications de smartphones et d'autres contenus sensibles. N'oubliez pas de retirer les cartes de stockage externes de vos appareils mobiles avant de vous en séparez (pour certains appareils, vos cartes SD peuvent être cachées dans le compartiment de la batterie voire éventuellement sous cette dernière). Ces cartes peuvent souvent être réutilisées dans de nouveaux équipements mobiles, ou même être utilisées comme stockage générique sur votre ordinateur via un adaptateur USB. Dans le cas où la réutilisation de votre carte SD n'est pas possible, alors, tout comme pour votre ancienne carte SIM, nous vous recommandons de la détruire physiquement.

Si vous n'êtes pas sûr de l'une des étapes abordées dans ce numéro, rendez-vous au magasin où vous avez acheté votre équipement mobile et sollicitez l'aide d'un technicien qualifié. Enfin, si vous jetez votre appareil mobile, nous vous prions d'envisager d'en faire don à la place. Il existe de nombreux organismes de bienfaisance qui acceptent les équipements mobiles usagés.

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.answersolutions.ch et http://answersecurity.com/

Ressources

NIST SP800-88 Rev. 1: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OUCH! Sauvegardes: http://answersecurity.com/2013/09/10/newsletter-ouch-septembre-2013/

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet