OUCH! | Février 2015

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

OUCH!

Dans ce numéro...



# Rester en sécurité sur la route

## Vue d'ensemble

Dans ce numéro, nous allons voir comment vous pouvez vous connecter à internet en toute sécurité lors de vos voyages.

## Rédacteur Invité

Steve Armstrong est le directeur technique de CyberCPR à Logically Secure, il est un instructeur certifié SANS et un ancien auteur de cours. Il est présent et actif sur Twitter sous le pseudo **@Nebulator** ainsi que sur Google +: **SteveArmstrongSecurity**.

## Repérage

Si votre réseau internet à la maison ou sur votre lieu de travail est sécurisé, lorsque vous voyagez, vous devez toujours partir du principe que quelque-soit le réseau auquel vous vous connectez, il n'est pas digne de confiance. Vous ne savez jamais qui d'autre est connecté en même temps que vous et à quelles menaces vous vous exposez. Quelques règles de base simples, avant votre voyage, peuvent protéger considérablement vos données lors de votre déplacement. Une ou deux semaines avant votre voyage :

- Identifiez quelles sont les données dont vous n'aurez pas besoin, sur les appareils que vous emportez, et retirez toute information non nécessaire. Ceci peut réduire considérablement l'impact dans le cas où vos appareils seraient volés, perdus ou saisis par la douane ou le personnel de sécurité des frontières. Si votre voyage est d'ordre professionnel, demandez à votre responsable si votre société fournit des appareils spécifiquement dédiés aux déplacements professionnels.
- Lors de voyages internationaux, pensez à vérifier quel type de connecteur d'alimentation utilise le pays dans lequel vous allez, il se peut que vous ayez besoin d'un adaptateur pour recharger vos appareils. De plus, vérifiez auprès de votre opérateur téléphonique de quel plan de service vous bénéficiez. Souvent, les opérateurs téléphoniques facturent des montants très élevés. En ce qui concerne l'utilisation des données à l'international, vous pourriez vouloir désactiver les fonctions d'échanges de données de votre téléphone lorsque vous voyagez à l'international, ou demander à votre opérateur téléphonique de vous fournir un plan de service valable pour l'international.
- Installez un logiciel sur votre appareil qui vous permet de le suivre et retrouver sa trace s'il venait à se perdre ou être volé, et qui vous permet également, dans ces cas-là, de le vider et effacer tout le contenu à distance. La plupart des appareils mobiles bénéficient de cette fonctionnalité, il vous suffira simplement de l'activer (mais rappelez-vous que vous aurez besoin d'un accès à internet pour ce faire).

Un ou deux jours avant votre voyage :

# Rester en sécurité sur la route

- Mettez à jour vos appareils, vos applications et vos anti-virus afin d'utiliser les dernières versions.
- Activez tous les paramètres de sécurité adéquats sur votre appareil, tels que vos firewalls.
- Verrouillez tous vos appareils mobiles avec des mots de passes forts ou des codes d'accès. De cette manière, si vous perdez votre appareil ou que l'on vous le vole, les gens ne pourront pas accéder à vos informations.
- Cryptez tous vos appareils afin que les données ne soient pas accessibles si l'appareil était perdu ou volé. Certains appareils, tel que les iPhones, font ceci automatiquement si vous installez un mot de passe ou un code d'accès sur l'appareil.
- Faîtes une sauvegarde complète de tous vos appareils. Ainsi si quelque chose leur arrivait, vous détenez toujours toutes vos données dans un autre endroit sécurisé.

*La clé pour être toujours en sécurité, même lorsque vous voyagez, est de sécuriser vos appareils avant de partir, les sécuriser physiquement et toujours savoir où ils se trouvent, à tout moment, et enfin crypter toute activité en ligne.*

## Appareils perdus / volés

Lorsque vous partez en voyage, assurez-vous de la sécurité physique de vos appareils. Par exemple, ne laissez jamais vos appareils en vue dans votre voiture, puisque les criminels vont simplement briser la vitre de votre voiture afin de s'emparer de tout objet de valeur. Vous pouvez tout à fait vous équiper d'un câble avec verrou ou d'un cadenas pour verrouiller physiquement vos appareils, tel que votre laptop, lorsque vous les laissez. Si le crime est clairement un risque, vous devez réaliser que vous avez plus de chances de perdre votre appareil que de vous le faire voler. Selon une étude menée sur dix ans par Verizon, les gens ont 15 fois plus de chances de perdre un appareil que de se le faire voler. De ce fait, pensez à toujours vérifier par deux fois que vous êtes toujours en possession de vos appareils lorsque vous voyagez, c'est-à-dire par exemple, lorsque vous passez la douane à l'aéroport, quittez un taxi ou un restaurant, quittez une chambre d'hôtel ou débarquez de l'avion.

## Accès Wi-Fi

Avoir accès à internet lorsque vous voyagez signifie souvent l'utilisation de points d'accès Wi-Fi publics, tels que ceux que l'on trouve dans un hôtel, un café ou à l'aéroport. Le problème avec ces points d'accès publics, c'est que non seulement vous ne savez pas qui les a installés mais vous ne savez pas non plus qui est en train de les utiliser en même temps que vous. C'est-à-dire que vous ne devez pas leur faire confiance, d'ailleurs c'est la raison pour laquelle vous avez effectué toutes les démarches décrites précédemment avant votre départ. De plus, le Wi-Fi utilise les ondes radios pour relier votre appareil au point d'accès sans fil. C'est dire que n'importe qui, présent physiquement non loin de vous, peut potentiellement intercepter et surveiller vos communications.

## Rester en sécurité sur la route

C'est pourquoi si vous utilisez le Wi-Fi public, vous devez impérativement vous assurer que votre activité online est cryptée. Par exemple, lorsque vous vous connectez, en utilisant votre navigateur, assurez-vous que les sites que vous visitez sont cryptés (l'URL est précédée de « https:// » et il doit y avoir un icône en forme de cadenas fermé). Aussi, vous possédez peut-être ce qu'on appelle un compte VPN (Virtual Private Network) qui se charge de crypter toutes vos activités en ligne. Ce compte a pu vous être délivré par votre travail ou vous pouvez acheter un accès VPN pour votre usage personnel. Si vous pensez ne pouvoir faire confiance à aucun point d'accès Wi-Fi, considérez l'option modem qu'offre votre smartphone. (Attention : ceci peut être très onéreux, comme expliqué précédemment, lorsque vous voyagez à l'international, pensez à vous rapprocher de votre fournisseur mobile pour davantage de renseignements avant votre départ.)

## Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

## 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

| | |
|---|---|
| Gestionnaires de mots de passe : | http://www.securingthehuman.org/ouch/2013#may2013 |
| Vérification en deux étapes : | http://www.securingthehuman.org/ouch/2013#august2013 |
| Chiffrement : | http://www.securingthehuman.org/ouch/2014#august2014 |
| Sécuriser votre nouvelle tablette : | http://www.securingthehuman.org/ouch/2013#december2013 |
| Verizon DBIR 2014 : | http://www.verizonenterprise.com/DBIR/2014/ |



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