OUCH! | Février, 2017

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

OUCH!

Dans ce numéro...

Voyager en toute sécurité

Vue d'ensemble

Nous voulons que vous puissiez tirer le meilleur de la technologie en tout temps, y compris quand vous voyagez. Dans ce numéro, nous vous expliquons comment vous pouvez vous connecter à Internet et utiliser vos périphériques en toute sécurité lors de vos déplacements.

Editeur invité

Mark Williams est l'architecte de sécurité de l'entreprise BlueCross Blueshield au Tennessee. Il est également instructeur SANS et président de l'association Chattanooga. Il a beaucoup voyagé et est particulièrement sensibilisé aux problèmes rencontrés lors de la prise en main de nouvelles technologies.

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 quel que soit le réseau auquel vous vous connectez, il n'est pas digne de confiance. En effet, vous ne savez jamais qui d'autre est connecté en même temps que vous et à quelles menaces vous vous exposez. Voici quelques règles de base simples à prendre en considération avant votre voyage qui peuvent protéger considérablement vos données lors de vos déplacements.

- Les informations les plus sûres sont les informations que vous n'avez pas. Identifiez les données dont vous n'avez pas besoin sur les appareils que vous apportez avec vous, puis supprimez ces informations. Cela peut réduire considérablement l'impact si vos appareils sont perdus, volés ou confisqués par la douane ou par la sécurité aux frontières. Si votre voyage est lié au travail, demandez à votre superviseur si votre organisation fournit des dispositifs qui sont utilisés spécifiquement pour travailler pendant le voyage.
- Verrouillez vos périphériques mobiles et / ou votre ordinateur portable avec un mot de passe ou un mot de passe fort. De cette façon, s'ils sont volés ou perdus, les gens ne peuvent pas accéder à vos informations à ce sujet. En outre, activez ou installez le chiffrement complet des disques sur vos appareils mobiles et portables. Pour la plupart des appareils mobiles, cela est automatiquement activé lorsque vous utilisez un screenlock.
- Installez ou activez le logiciel sur votre appareil afin de pouvoir localiser à distance votre périphérique et même d'effacer le contenu à distance s'il a été perdu ou volé.
- Mettez à jour vos périphériques, applications et logiciels anti-virus avant de partir afin d'exécuter les dernières versions. Beaucoup d'attaques se concentrent sur les systèmes avec des logiciels obsolètes.
- Effectuez une sauvegarde complète de tous vos périphériques. De cette façon, si quelque chose leur arrive lors du

Voyager en toute sécurité

voyage, vous avez toujours toutes vos données d'origine dans un endroit sécurisé.

- Pour les voyages internationaux, vérifiez le plan de service que vous avez souscrit auprès de votre fournisseur de services mobiles. Souvent, les fournisseurs de services facturent des tarifs élevés pour l'utilisation de données internationales, vous pouvez désactiver vos capacités de données cellulaires lors d'un voyage international ou acheter une carte SIM prépayée locale conçue pour des voyages internationaux.

Pour voyager en toute sécurité, sécurisez vos appareils avant de partir. Sécurisez-les physiquement et chiffrez toutes vos activités 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 dans votre voiture où les gens peuvent facilement les voir : les criminels peuvent simplement briser la fenêtre de votre voiture et saisir quelque chose de valeur qu'ils peuvent voir. Alors que le crime est certainement un risque, selon une récente étude de Verizon, les gens sont 100 fois plus susceptibles 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. Par exemple, lorsque vous passez la douane à l'aéroport, quittez un taxi ou un restaurant, quittez une chambre d'hôtel ou encore débarquez d'un avion. Dans ce dernier cas de figure, n'oubliez pas de vérifier la poche arrière du siège de l'avion!

Accès Wi-Fi

Avoir accès à Internet lorsque vous voyagez signifie souvent utiliser des points d'accès Wi-Fi publics, comme ceux que vous trouverez dans un hôtel, un café ou dans un aéroport. Deux problèmes se posent avec le Wi-Fi public: vous ne savez jamais qui a configuré ces accès et vous ne savez jamais qui est connecté. En tant que tels, ils doivent être de ce fait considérés comme non fiables. En fait, c'est la raison pour laquelle vous avez pris toutes les mesures pour sécuriser vos périphériques avant votre départ. Par ailleurs, le Wi-Fi utilise des ondes radio pour relier votre appareil au point d'accès sans fil, ce qui signifie que quiconque physiquement près de vous peut potentiellement intercepter et surveiller ces communications. C'est pourquoi si vous utilisez le Wi-Fi public, vous devez impérativement vous assurer que votre activité en ligne est chiffrée. Par exemple, lorsque vous vous connectez, en utilisant votre navigateur, assurez-vous que les sites que vous visitez soient chiffrés (l'URL est précédée de « https:// » et il doit y avoir un icône en forme de cadenas fermé). Aussi, vous possédez peut être ce que l'on appelle un compte VPN (Virtual Private Network) qui se charge de chiffrer toutes vos activités en ligne.

Voyager en toute sécurité

Ce compte a pu vous être délivré dans le cadre de votre travail. Il est également possible d'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. Cependant, cela peut s'avérer être très coûteux. 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 pas d'ordinateurs publics, comme ceux mis à disposition dans les halls d'hôtels ou des cybercafés, pour vous connecter à un compte ou accéder à des informations sensibles. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, n'oubliez pas qu'il est possible 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 faites confiance pour vos activités en ligne. Si vous n'avez pas 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.answer.ch et http://answersecurity.com/

Sources

Phrases de passe :	https://securingthehuman.sans.org/ouch/2015#april2015
Sauvegardes :	https://securingthehuman.sans.org/ouch/2015#august2015
Malware :	https://securingthehuman.sans.org/ouch/2016#march2016
Chiffrement :	https://securingthehuman.sans.org/ouch/2016#june2016
Archives OUCH! / Traduction :	https://securingthehuman.sans.org/ouch/archives

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet