OUCH! | Mai 2015

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

OUCH!

Dans ce numéro...

- Vue d'ensemble
- Les bases
- Jeunes enfants

Sécuriser le cyber espace pour le fossé des générations

Vue d'ensemble

Beaucoup d'entre nous se sentent à l'aise avec la technologie, y compris sur la manière de l'utiliser en toute sécurité. Cependant, d'autres membres de votre famille peuvent ne pas se sentir totalement à l'aise avec la technologie, surtout s'ils n'ont pas grandi avec des ordinateurs ou Internet. Voici quelques mesures que vous pouvez prendre en considération pour aider à sécuriser le fossé des générations. En outre, vous pouvez prendre des mesures pour sécuriser vos enfants à la maison, cependant, des mesures de sécurité similaires peuvent ne pas exister lorsque vos enfants rendent par exemple visite à un parent. De ce fait, nous aborderons également comment vous pouvez aider à créer un environnement en ligne plus sûr quand vos enfants rendent visite à ces parents.

Rédacteur Invité

Brian Honan (Twitter **@brianhonan**) est un consultant en sécurité indépendant basé à Dublin en Irlande. Il est également le fondateur du CERT en Irlande, le centre européen de lutte contre la cybercriminalité (EC3), dont il est à la tête. Il donne aussi des conférences sur la sécurité à l'université de Dublin. Auteur de nombreux livres, il écrit également des publications pour diverses industries.

Les bases

Ces quelques étapes de base, peuvent permettre d'assurer la vie numérique de chacun. Voici les mêmes étapes de base que nous recommandons toujours pour tout membre de votre famille. Toutefois, si vous connaissez un membre de votre famille qui ne comprend pas ces étapes, vous serez peut être amené à les mettre en place vous-même.

- **Ingénierie sociale**: Expliquer le concept d'ingénierie sociale en termes simples afin que tout le monde puisse s'y identifier. Les escroqueries et les escrocs existant depuis des milliers d'années, ces types d'attaques ne sont pas nouvelles. La seule différence est que maintenant les criminels appliquent ces mêmes concepts au travers d'Internet. Donnez des exemples d'attaques les plus courantes d'aujourd'hui, comme les e-mails de phishing communs ou les arnaques du support technique de Microsoft. Assurez-vous que les membres de votre famille comprennent qu'ils ne doivent jamais donner leur mot de passe à quiconque ou permettre l'accès à distance à leur ordinateur. Enfin, assurez-vous qu'ils savent que s'ils se sentent mal à l'aise ou ont des questions au sujet d'un email ou encore que quelqu'un les contacte, qu'ils peuvent faire appel à vous avant de communiquer toute information.
- **Accueil réseau Wi-Fi**: Prenez le temps de vous assurer que le réseau Wi-Fi de leur domicile est sécurisé. Assurez-vous au minimum que le mot de passe admin par défaut a été changé, il doit y avoir un mot de passe fort pour accéder au réseau Wi-Fi, et la connexion réseau doit utiliser le dernier cryptage. Vous pouvez aussi envisager de configurer le réseau Wi-Fi pour utiliser un formulaire sécurisé de DNS tels que les Services DNS sécurisés www.opendns.org. de façon à ce que cela puisse non seulement empêcher les gens de visiter des sites Web infectés, mais puisse également vous donner le contrôle sur les sites web que les gens peuvent ou ne

Sécuriser le cyber espace pour le fossé des générations

peuvent pas visiter. Cela peut s'avérer utile pour les sites web que les enfants visitent.

- **Patching**: Garder les systèmes actuels et entièrement mis à jour est une des étapes les plus fondamentales que vous pouvez prendre en considération pour assurer n'importe quelle technologie. En tant que tel, assurez-vous que tous les appareils de la maison (y compris les appareils mobiles) et les applications soient entièrement patchés. La façon la plus simple d'y parvenir est de permettre la mise à jour automatique dans la mesure du possible.
- **Anti-Virus**: Les gens font des erreurs. En effet, nous cliquons parfois ou installons des choses que nous ne devrions probablement pas installer ou sur lesquelles nous ne devrions pas cliquer. Un anti-virus ne peut pas arrêter tous les programmes malveillants, il peut en revanche vous aider à détecter et arrêter les attaques les plus courantes. En tant que tel, assurez-vous que tous les ordinateurs de la maison soient dotés d'un anti-virus, et que ce dernier soit à jour et actif.

Les générations plus âgées peuvent avoir besoin d'aide au niveau de la sécurisation de leur technologie à la maison et ainsi créer un environnement sûr pour tous les visiteurs y compris les plus jeunes enfants.

- **Les mots de passe**: Les mots de passe forts veillent essentiellement à protéger à la fois les appareils et les comptes en ligne. Expliquez aux membres de votre famille la façon de créer des mots de passe forts. Les phrases de passe peuvent être plus faciles pour eux à utiliser et à mémoriser. Une autre idée est d'installer un gestionnaire de mot de passe et de leur apprendre à l'utiliser. Si cela ne fonctionne pas, apprenez leur peut être à écrire leurs mots de passe, puis stocker ces mots de passe dans un endroit sûr où seulement eux puissent accéder. Pour tous les comptes en ligne critiques, vous pouvez également mettre en place une vérification en deux étapes.
- **Sauvegardes**: Quand tout le reste échoue, les sauvegardes sauront sauver la situation. Assurez-vous que les membres de votre famille disposent d'un système de sauvegarde de fichiers simple et fiable.

Vous pouvez également faire une vérification mensuelle ou trimestrielle pour vous assurer que toutes ces étapes sont en place. Dans le pire des cas, considérez l'installation du logiciel d'administration à distance sur un périphérique, cependant, si vous voulez être certain que cela soit vraiment sûr, dans ce cas, utilisez le chiffrement et un mot de passe fort unique.

Enfants en visite

Très souvent, lorsque de jeunes enfants se rendent chez un parent, comme par exemple leurs grands-parents, les règles en vigueur chez vous ne peuvent plus s'appliquer. Cela peut inclure des règles visant à aider à protéger vos enfants en ligne. Voici quelques mesures que vous pouvez prendre pour aider à protéger les enfants.

- **Règles** : Assurez-vous que les parents chez qui sont vos enfants, connaissent les règles ou les attentes que vous avez en matière de sécurité. Par exemple, y at-il des règles sur la façon dont les enfants peuvent jouer en ligne ou

Sécuriser le cyber espace pour le fossé des générations

quand peuvent-ils avoir accès à leurs appareils mobiles? Faites-nous confiance, ne comptez pas sur vos enfants pour expliquer les règles à leurs grands-parents ou à d'autres membres de votre famille. Une idée est d'établir une «feuille de règles» et de la partager avec des parents où votre enfant se rend fréquemment.

- **Contrôle**: Si vos enfants comprennent la technologie mieux que leurs grands-parents, ils peuvent en prendre avantage. Par exemple, les enfants peuvent demander ou obtenir des droits administratifs sur l'ordinateur de leurs grands-parents, puis faire ce qu'ils veulent, comme l'installation d'un jeu auquel vous ne voulez pas qu'ils jouent. Assurez-vous dans ce cas que les grands-parents comprennent qu'il ne faut pas donner aux enfants tout accès supplémentaire au-delà de ce qui a été établi.

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/

Sources

Ingénierie sociale :	http://www.securingthehuman.org/ouch/2014#november2014
Sécuriser votre réseau domestique :	http://www.securingthehuman.org/ouch/2014#january2014
Phrases de passe :	http://www.securingthehuman.org/ouch/2015#april2015
Qu'est-ce qu'un Anti-Virus ? :	http://www.securingthehuman.org/ouch/2014#december2014
Protéger vos enfants en ligne :	http://www.securingthehuman.org/ouch/2013#april2013
Support pour les arnaques au téléphone :	http://www.onguardonline.gov/articles/0346-tech-support-scams
Création d'un cyber espace sécurisé :	http://www.securingthehuman.org/resources/posters

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