OUCH! | Octobre 2017

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

OUCH!

Dans ce numéro...

Aider les autres à se protéger par eux-mêmes

Vue d'ensemble

Beaucoup d'entre nous se sentent à l'aise avec la technologie et comprennent comment l'utiliser de façon sûre et sécurisée. Cependant, certains de vos amis ou membres de votre famille ne se sentent pas forcément si à l'aise. En fait, ils peuvent être confus, intimidés ou même effrayés par la technologie. Cela les rend très vulnérables aux yeux des cyber-attaquants d'aujourd'hui. La cybersécurité ne doit pas être effrayante, elle est même plutôt simple une fois que vous en comprenez les bases. Les membres de votre entourage que cela effraie ont tous probablement besoin d'un guide comme vous pour les aider à comprendre les bases.

Editeur invité

Randy Marchany (Twitter: **@randymarchany**) est le CISO de Virginia Tech et est un instructeur certifié du SANS Institute.

Cinq étapes simples

Voici cinq étapes simples que vous pouvez prendre en considération pour aider votre entourage à surmonter leurs peurs et à tirer pleinement parti de la technologie d'aujourd'hui. Pour plus d'informations sur chacun de ces points, reportez-vous à la section Références à la fin de cette newsletter.

1. **Ingénierie sociale** : l'ingénierie sociale est une technique courante utilisée par les cyber-agresseurs pour tromper ou inciter les gens à faire quelque chose qu'ils ne devraient pas faire, comme par exemple partager leur mot de passe, infecter leur ordinateur ou partager des informations sensibles. Ce n'est pas nouveau, les escroqueries et les escrocs existent depuis des milliers d'années. La seule différence maintenant est que les criminels appliquent ces mêmes concepts à Internet. Vous pouvez assister les autres en les aidant à repérer les indices les plus courants d'une attaque d'ingénierie sociale, comme par exemple, lorsque quelqu'un crée un énorme sentiment d'urgence, quand quelque chose est trop beau pour être vrai, ou encore quand un cyber-attaquant prétend être quelqu'un que vous connaissez, mais que leurs messages ne ressemblent pas à ceux d'un de vos amis. Partagez des exemples d'attaques communes d'ingénierie sociale, telles que les courriels d'hameçonnage ou les faux appels téléphoniques de Microsoft Tech-Support. Si vous ne disposez de rien d'autre, assurez-vous que les membres de votre entourage comprennent qu'ils ne devraient jamais donner leur mot de passe à personne ou autoriser l'accès à distance à leur ordinateur.
2. **Mots de passe** : les mots de passe forts sont essentiels pour protéger les périphériques et les comptes en ligne. Accompagnez votre entourage à travers la façon de créer des mots de passe forts. Nous recommandons les mots de passe, car ils sont les plus faciles à saisir et à se rappeler. Les phrases de passe ne sont que des mots de passe composés

Aider les autres à se protéger par eux-mêmes

de plusieurs mots. Aidez également votre entourage à installer et à utiliser un gestionnaire de mot de passe. Il est important d'avoir un mot de passe unique pour chacun de vos appareils et comptes. Si un gestionnaire de mot de passe leur semble contraignant, apprenez-leur dans ce cas à écrire leurs mots de passe, puis à les stocker dans un emplacement sécurisé. Enfin, pour les comptes importants, aidez-les à activer la vérification en deux étapes (souvent appelée authentification à deux facteurs). La vérification en deux étapes est l'une des étapes les plus efficaces dont vous pouvez vous servir pour sécuriser chacun de vos comptes.

Aidez les autres à tirer le meilleur parti de la technologie en partageant avec eux ces cinq étapes simples.

3. **Patching**: garder ses systèmes entièrement à jour est une étape clé que tout le monde peut prendre en considération pour sécuriser ses appareils. Ceci n'est pas seulement valable pour vos ordinateurs et appareils mobiles, mais aussi pour tout ce qui est connecté à Internet, comme les consoles de jeu, les thermomètres ou même les lumières ou les haut-parleurs. La façon la plus simple de s'assurer que tous les appareils soient à jour est d'activer leur mise à jour automatique chaque fois que cela est possible.
4. **Anti-Virus**: les gens font des erreurs, nous installons et cliquons parfois sur des choses sur lesquelles nous ne devrions probablement pas et qui peuvent infecter nos systèmes. Un anti-virus est conçu pour nous protéger de ces erreurs. Alors que l'antivirus ne peut pas arrêter tous les logiciels malveillants, il aide cependant à détecter et à arrêter les attaques les plus courantes. En tant que tel, assurez-vous que les ordinateurs domestiques ont un antivirus installé et qu'il est actuel et actif. En outre, bon nombre des solutions d'anti-virus d'aujourd'hui incluent d'autres technologies de sécurité telles que les pare-feux et la protection du navigateur.
5. **Sauvegardes** : lorsque tout le reste échoue, les sauvegardes sont souvent la seule façon de récupérer des erreurs telles que la suppression de fichiers erronés ou des cyber-attaques telles que le Ransomware. Assurez-vous que votre famille et vos amis disposent d'un système automatisé de sauvegarde de fichiers en place. Souvent, les solutions les plus simples sont basées sur le Cloud, qui sauvegardent vos périphériques chaque heure ou chaque fois que vous modifiez un fichier. Ces solutions facilitent non seulement la sauvegarde des données, mais les récupèrent également.

Sécuriser les enfants lors de leurs visites chez les autres

Si vous êtes à l'aise avec la technologie, il est fort probable que vous n'êtes pas le seul à devoir être sécurisé, et que vous devez également sécuriser vos enfants. Cependant, lorsque les enfants rendent visite à un parent qui n'est pas à l'aise avec la technologie, comme leurs grands-parents par exemple, ces derniers peuvent ne pas être conscients de la meilleure façon de protéger leurs petits enfants en ligne ou en adéquation avec vos attentes. Voici quelques étapes que vous pouvez exécuter pour protéger vos enfants lorsqu'ils rendent visite à d'autres personnes, en particulier à des membres de votre famille.

Aider les autres à se protéger par eux-mêmes

- **Règles**. Assurez-vous que s'il existe des règles ou des attentes que vous avez pour la sécurité de votre enfant, d'autres les connaissent. Par exemple, y a-t-il des règles concernant la durée pendant laquelle vos enfants peuvent être en ligne, à qui peuvent-ils parler ou à quels jeux peuvent-ils ou ne peuvent-ils pas jouer ? Faites-nous confiance, ne pensez pas que les enfants expliquent les règles à d'autres membres de la famille. Une astuce simple et efficace consiste à créer une « feuille de règles » et de la partager lors de visites fréquentes de votre enfant.
- **Contrôle**: si un enfant comprend mieux la technologie que les personnes qui le gardent, il peut en profiter. Par exemple, les enfants peuvent demander ou obtenir des droits administratifs sur l'ordinateur d'un grand-parent et faire tout ce qu'ils veulent, comme installer un jeu auquel vous ne voulez peut-être pas qu'ils jouent. Assurez-vous que les parents comprennent que cela ne devrait pas donner aux enfants un accès supplémentaire au-delà de ce qui a été établi.

Enfin, suggérez aux personnes de prendre connaissance de références comme la newsletter l'OUCH! afin qu'ils puissent continuer à apprendre par eux-mêmes. Cette newsletter est publiée chaque mois gratuitement dans plus de 20 langues. Inscrivez-vous à https://securingthehuman.sans.org/ouch.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Sources

Ingénierie sociale :	https://securingthehuman.sans.org/ouch/2017#january2017
Phrases de passe :	https://securingthehuman.sans.org/ouch/2017#april2017
Gestionnaire de mots de passe :	https://securingthehuman.sans.org/ouch/2017#september2017
Vérification en deux étapes :	https://securingthehuman.sans.org/ouch/2015#september2015
Sauvegarde et récupération :	https://securingthehuman.sans.org/ouch/2017#august2017
Sécuriser les enfants en ligne d'aujourd'hui :	https://securingthehuman.sans.org/ouch/2017#may2017

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet