OUCH! | Octobre 2016

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

OUCH!

Dans ce numéro...

Quatre étapes pour se sécuriser

Apercu

Alors que la technologie prend un rôle de plus en plus important dans notre quotidien, celle-ci se complexifie également. Etant donné l'évolution rapide des technologies, se souvenir de toutes les bonnes pratiques liées à la sécurité n'est pas évident. Il semble toujours y avoir de nouveaux conseils sur ce qu'il convient de faire. Toutefois même si les détails peuvent changer, certains fondamentaux seront toujours les mêmes pour vous protéger. Indépendamment des technologies que vous utilisez, nous vous recommandons les quatre étapes clés suivantes. Si vous souhaitez plus d'informations sur ces étapes, vous pouvez consulter les sources données à la fin de cet article.

Editeur invité

L'objectif de Ryan Johnson est de s'assurer que les sociétés sont prêtes à répondre aux inévitables brèches de sécurité pouvant survenir. Il enseigne des techniques avancées d'analyse Forensic à l'institut SANS. Vous pouvez suivre Ryan sur Twitter **@ForensicRJ**.

1. **Vous**: Dans un premier temps, vous devez absolument garder en tête que la technologie seule ne pourra pas complétement vous protéger. Les attaquants ont appris que le moyen le plus facile de contourner même les technologies de sécurité les plus avancées est de s'attaquer à vous. S'ils souhaitent obtenir votre mot de passe, votre numéro de carte de crédit ou autres données personnelles, le plus simple est de vous duper afin que vous leur donniez l'information. Par exemple, ils peuvent vous appeler en se faisant passer pour un technicien Microsoft et prétendre que votre ordinateur est infecté. En réalité cette personne est un cybercriminel souhaitant avoir un accès à votre ordinateur. Un attaquant peut également vous envoyer un email vous expliquant qu'un paquet à livrer est bloqué et que la seule façon de le débloquer est de confirmer votre adresse en suivant le lien présent dans le mail. En réalité il cherche à vous pousser à visiter un site malicieux pouvant compromettre votre ordinateur. C'est d'ailleurs comme ça que commencent les attaques Ransomware ou la fraude au président. Au final, vous êtes la meilleure défense face à une attaque. En utilisant votre bon sens vous pouvez identifier et bloquer la plupart des attaques.

2. **Les mots de passe**: La prochaine étape pour vous protéger, est d'utiliser un mot de passe fort et unique pour chacun de vos terminaux et comptes en ligne. L'emphase est réellement sur les mots « Fort » et « Unique ». Un

Quatre étapes pour se sécuriser

mot de passe qui est fort ne pourra pas être facilement deviné par un hacker ou un de leurs programmes automatisés. Par contre, vous en avez marre de devoir vous souvenir de mots de passe complexes et difficiles à taper ? Essayer d'utiliser une phrase. A la place d'un mot unique vous pouvez utiliser une suite de mots qui est plus facile à retenir, par exemple : « Ou est mon café ? ». Plus longue est la phrase, plus c'est sécurisé. Un mot de passe unique signifie un mot de passe par terminal et application. De cette façon, si l'un de vos mots de passe est compromis, le reste de vos comptes et terminaux restent en sécurité. Vous n'arrivez pas à vous souvenir de tous vos mots de passe ? Pas d'inquiétude, nous non plus ! C'est pourquoi nous vous recommandons l'utilisation d'un gestionnaire de mots de passe. C'est un outil dédié qui permet de sauvegarder de manière sécurisé vos mots de passe. Celui-ci stock de façon chiffré vos mots de passe sur votre ordinateur ou téléphone portable.

En prenant en compte ces quatre éléments clés vous pourrez vous protéger tout en continuant à utiliser les dernières technologies.

Pour finir, ce que vous pouvez faire de plus important pour protéger votre compte est d'activer l'authentification en deux étapes. Les mots de passe ne sont plus suffisant pour protéger vos comptes, il faut quelque chose de plus fort. L'authentification en deux étapes est beaucoup plus forte. Elle utilise toujours le mot de passe mais y ajoute une deuxième authentification. Que celle-ci soit qui vous êtes (biométrie) ou ce que vous possédez (par exemple un code envoyé ou généré sur votre téléphone portable). Nous vous conseillons d'activer cette option sur tous les comptes que vous avez, en particulier sur votre gestionnaire de mot de passe. L'authentification en deux étapes est probablement l'étape la plus importante que vous puissiez mettre en place pour vous protéger et c'est bien plus simple que ce que vous pouvez imaginer.

3. **Les mises à jour**: Faites-en sorte que votre ordinateur, votre mobile ainsi que tous vos objets connectés à internet bénéficient de la dernière version de leur logiciel. En effet, les cybercriminels recherchent constamment de nouvelles vulnérabilités dans les softwares qu'utilisent vos objets. Lorsqu'une telle vulnérabilité est découverte, ils utilisent des programmes spécifiques pour les exploiter et hacker vos terminaux. Dans le même temps, les sociétés éditrices travaillent constamment pour bloquer les vulnérabilités en publiant régulièrement des mises à jours. En gardant vos

Quatre étapes pour se sécuriser

terminaux à jour, vous compliquez la tâche des pirates souhaitant s'en prendre à vous. N'hésitez pas à activer les mises à jours automatique dès que possible. Cette règle s'applique à toutes les technologies connectées à un réseau, les ordinateurs, les routeurs, les caméra IP et bientôt même votre voiture. Si votre OS ou terminal n'est plus supporté et n'a donc pas de mise à jour de sécurité, nous vous recommandons d'en changer.

4. **Les Sauvegardes**: Parfois, alors même que toutes les précautions sont prises, vous pouvez être piraté. Si c'est le cas, votre seule option est souvent de tout effacer sur votre terminal afin de vous assurer qu'il ne soit plus infecté. L'attaquant peut également vous empêcher d'accéder à vos fichiers personnels, photos ou autres. La seule façon de tout restaurer est d'avoir une sauvegarde. Prenez soin de faire régulièrement des sauvegardes de toutes vos données importantes et vérifiez que ces sauvegardes fonctionnent. La plupart des OS et des terminaux peuvent faire des backups automatiques. De plus nous vous recommandons de stocker vos sauvegardes dans le cloud ou hors ligne afin de les protéger de attaques.

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

Phishing :	https://securingthehuman.sans.org/ouch/2015#december2015
Gestionnaire de mots de passe :	https://securingthehuman.sans.org/ouch/2015#october2015
La double authentification :	https://securingthehuman.sans.org/ouch/2015#september2015
Phrases de passe :	https://securingthehuman.sans.org/ouch/2015#april2015
Les sauvegardes :	https://securingthehuman.sans.org/ouch/2015#august2015

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