OUCH! | Octobre 2014

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

OUCH!

Dans ce numéro...

Cinq étapes pour rester sécurisé

Vue d'ensemble

Si la technologie joue un rôle de plus en plus important dans notre vie quotidienne, elle gagne également en complexité. Compte tenu de la vitesse à laquelle elle évolue, rester à jour sur des conseils en matière de sécurité peut s'avérer délicat. Il semble qu'il y ait constamment de nouvelles directives sur ce qu'il convient de faire ou ne pas faire. Cependant, si certains détails changent au fil du temps, il existe tout de même certaines bases fondamentales sur lesquelles vous appuyez pour vous aider à vous protéger. Indépendamment de quelle technologie vous utilisez et où vous l'utilisez, nous vous recommandons de suivre ces 5 étapes clés.

Editeur invité

Lenny Zeltser se concentre essentiellement sur la protection des opérations informatiques de ses clients à NCR Corp et enseigne comment combattre les logiciels malveillants au SANS Institute. Lenny est présent sur twitter **@lennyzeltser** et tient un blog **blog.zeltser.com**.

Cinq étapes clés

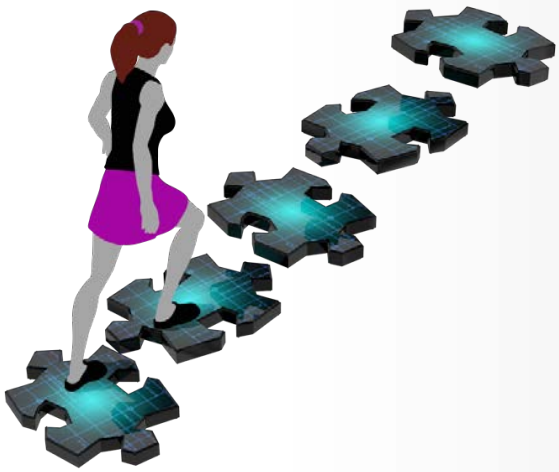
Chacune des 5 étapes ci-dessous est une simple vue d'ensemble. Pour en apprendre davantage sur chaque étape, veuillez-vous référer à la section Ressources, au bas de ce numéro.

1. **Vous** : D'abord et avant tout, gardez bien à l'esprit que la technologie seule ne vous protègera pas. Les agresseurs ont bien compris que la meilleure des solutions pour contourner les technologies de sécurité consiste à vous attaquer, vous. S'ils cherchent à obtenir votre mot de passe ou numéro de carte de crédit, ils vont vous incitez, par quelque subterfuge, à leur révéler ces informations. Par exemple, ils peuvent vous contacter en se faisant passer pour le support technique Microsoft et en vous disant que votre ordinateur est infecté, alors qu'en réalité, ce ne sont que des cybers criminels qui cherchent à y avoir accès. Ou ils peuvent éventuellement vous envoyer un mail pour vous dire qu'un colis n'a pas pu vous être livré et vous demander de cliquer sur un lien pour confirmer votre adresse, alors qu'en réalité, il s'agit d'un site malveillant qui va pirater votre ordinateur. Finalement, la meilleure défense contre les agresseurs, c'est vous. Méfiez-vous, et avec un peu de bon sens, vous pourrez ainsi repérer et éviter la plupart des attaques.

2. **Mise à jour** : Assurez-vous que vous utilisez bien la dernière version du logiciel sur vos ordinateurs, dispositifs portables, applications ou toute autre appareil connecté. Les cybers criminels sont sans cesse à la recherche de failles dans les systèmes que vous utilisez. Lorsqu'ils découvrent les faiblesses, ils utilisent un programme spécial pour abuser de la vulnérabilité et pirater n'importe quelle de vos technologies, votre réseau, votre ordinateur ou dispositifs mobiles.

Cinq étapes pour rester sécurisé

Dans le même temps, les entreprises, qui ont créés la technologie que vous utilisez, travaillent dur à effectuer et maintenir les mises à jour. Dès qu'une faille a été découverte, ils créent un correctif et le communiquent aux utilisateurs. En vous assurant de la mise à jour de vos ordinateurs et dispositifs mobiles, vous réduisez considérablement le nombre de failles, rendant ainsi beaucoup plus compliqué le piratage éventuel. Pour rester à jour, autorisez, dès que possible, toute mise à jour automatique. Cette règle s'applique à presque tous les systèmes technologiques connectés à un réseau, y compris les téléviseurs connectés à Internet, les interphones pour bébés, les routeurs domestiques, les consoles de jeux ou même, pourquoi pas un jour, votre voiture. Si le système d'exploitation de votre ordinateur, vos dispositifs mobiles ou toute autre technologie que vous utilisez n'est plus soutenue et ne reçoit plus les mises à jour, nous vous recommandons d'acquérir une version plus récente qui sera soutenue par le fournisseur.



En suivant ces 5 étapes clés, et grâce aux nouvelles technologies, vous contribuerez grandement à vous protéger.

3. **Mots de passe** : L'étape suivante pour vous protéger consiste en l'utilisation d'un mot de passe unique et fiable pour chacun de vos appareils, comptes en ligne et applications. Les mots clés à retenir ici sont unique et fiable. Un mot de passe sécurisé signifie qu'il ne doit pas être facilement deviné par les pirates ni par leurs programmes automatisés. Au lieu d'un simple mot, utilisez une longue phrase composée de plusieurs mots, et ajoutez-y des symboles et des chiffres pour faire bonne mesure. Un mot de passe unique signifie qu'il doit être différent pour chacun de vos appareils et comptes en ligne. De cette manière, si l'un de vos mots de passe était compromis, tous vos autres comptes seraient toujours sécurisés. Vous ne vous souvenez pas de tous ces mots de passe uniques et sécurisés ? Ne vous inquiétez pas, nous non plus ! C'est pourquoi nous vous recommandons l'utilisation d'un gestionnaire de mot de passe, une application spécialisée pour votre smartphone ou ordinateur, qui stocke tous vos mots de passe de manière sécurisée dans un format crypté. Enfin, si vos comptes en ligne vous proposent un système de double vérification, nous vous recommandons vivement de l'installer puisqu'il s'agit là d'une des meilleures façons de protéger votre compte.

4. **Cryptage (encryptage) / encodage** : Une troisième étape que nous recommandons est l'encodage. L'encodage vous assure que seule vous et les personnes à qui vous faites confiance peuvent avoir accès à vos informations. Les données peuvent être cryptées dans deux « endroits » : stockées ou en cours de transfert. Crypter les données au repos signifie les protéger alors qu'elles sont stockées sur votre ordinateur sous forme de dossier ou sur une clé USB. La plupart des systèmes d'exploitation vous permettent d'encoder automatiquement toutes vos données en utilisant

Cinq étapes pour rester sécurisé

des fonctions telles que « Full Disk Encryption » (= cryptage total du disque ?). Nous vous recommandons d'autoriser cela dès que possible. Crypter les données « en mouvement » signifie crypter les données lors de leur transfert, lors de l'utilisation de vos services bancaires en ligne, par exemple. Une manière simple de vérifier que l'encodage est activée lorsque vous surfez consiste à vous assurer que l'adresse du site que vous êtes en train de visiter commence bien par « https » et qu'il y a une petite icône représentant un cadenas, à côté.

5. **Sauvegardes** : Quelques fois, malgré tous vos efforts, un de vos appareils ou comptes peut se trouver compromis. Dans ce cas, souvent, la seule solution pour vous assurer que votre ordinateur ou votre téléphone mobile ne contient pas de virus, est de tout effacer et recommencer à zéro. Le pirate peut même éventuellement vous empêcher d'accéder à vos dossiers personnels, photos ou autres informations stockées sur le système compromis. Votre unique option sera peut-être de restaurer toute vos informations personnelles grâce à une sauvegarde. Assurez-vous que vous faîtes régulièrement des sauvegardes et, surtout, que vous êtes en mesure de les utiliser pour restaurer votre ordinateur. La plupart des systèmes d'exploitation et appareils mobiles permettent des sauvegardes automatiques.

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

Mots de passe forts:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_fr.pdf
Gestionnaires de mots de passe:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_fr.pdf
Sauvegardes:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_fr.pdf
Termes de sécurité:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_fr.pdf
Gestionnaires de mots de passe:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_fr.pdf
Sauvegardes:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_fr.pdf
Termes de sécurité:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_fr.pdf

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