SANS SECURITY AWARENESS
Pélissier & Partners
Explorateurs de connaissances

OUCH! | Janvier 2018

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

OUCH!

Dans ce numéro...

Créer une maison Cyber-sécurisée

Vue d'ensemble

Il y'a quelques années, créer une maison cyber-sécurisée était simple; la plupart des maisons ne comportaient rien de plus qu'un réseau sans fil et plusieurs ordinateurs. Aujourd'hui, la technologie est devenue beaucoup plus complexe et est intégrée dans toutes les parties de notre vie quotidienne : des appareils mobiles et des consoles de jeu à votre thermostat et même peut-être votre réfrigérateur. Voici quatre étapes simples pour créer une maison cyber-sécurisée.

Editeur invité

Matt Bromiley est un répondeur d'incident de jour où il aide les clients de toutes tailles à gérer les violations de données. Il est également instructeur SANS et enseigne FOR508, le cours avancé de criminalistique numérique et d'intervention en cas d'incident. Suivez Matt **@mbromileyDFIR**.

Votre réseau sans fil

Presque tous les réseaux domestiques commencent par un réseau sans fil (ou Wi-Fi). C'est ce qui permet à tous vos appareils de se connecter à Internet. La plupart des réseaux sans fil à domicile sont contrôlés par votre routeur Internet ou par un point d'accès sans fil distinct dédié. Ils fonctionnent tous deux de la même manière en diffusant des signaux sans fil, les appareils de votre maison se connectent via ces signaux. Cela signifie que la sécurisation de votre réseau sans fil est un élément clé de la protection de votre maison. Nous recommandons les étapes suivantes pour le sécuriser.

- Modifiez le mot de passe administrateur par défaut pour votre routeur Internet ou votre point d'accès sans fil, selon la commande de votre réseau sans fil. Le compte administrateur est ce qui vous permet de configurer les paramètres pour votre réseau sans fil.
- Assurez-vous que seules les personnes de confiance peuvent se connecter à votre réseau sans fil. Pour ce faire, en permettant une sécurité renforcée. Actuellement, la meilleure option consiste à utiliser le mécanisme de sécurité appelé WPA2. En l'activant, un mot de passe est requis pour que les gens puissent se connecter à votre réseau domestique, et une fois connectés, leurs activités en ligne sont cryptées.
- Assurez-vous que le mot de passe utilisé pour vous connecter à votre réseau sans fil est un mot de passe fort et qu'il est différent du mot de passe administrateur. Rappelez-vous que vous n'avez pas besoin d'entrer le mot de passe qu'une fois pour chacun de vos appareils, car ils stockent et mémorisent le mot de passe.

Créer une maison Cyber-sécurisée

- De nombreux réseaux sans fil prennent en charge ce que l'on appelle un réseau invité. Cela permet aux visiteurs de se connecter à Internet, mais protège votre réseau domestique car ils ne peuvent pas se connecter à l'un des autres périphériques de votre réseau domestique. Si vous ajoutez un réseau invité, veillez à activer WPA2 ainsi qu'un mot de passe unique pour ce réseau.

Vous ne savez pas comment exécuter ces étapes? Demandez à votre fournisseur d'accès Internet ou consultez leur site Web. Vous pouvez aussi consulter la documentation fournie avec votre routeur Internet ou votre point d'accès sans fil ou consulter leur site Web respectif.

Suivez ces quatre étapes simples pour créer une maison cyber-sécurisée; sécurisez votre réseau Wi-Fi, activez la mise à jour automatique, utilisez des mots de passe uniques et activez les sauvegardes.

Vos appareils

L'étape suivante consiste à savoir quels périphériques sont connectés à votre réseau domestique sans fil et à vous assurer que tous ces périphériques sont sécurisés. Cela était simple quand vous n'aviez qu'un ordinateur ou deux. Cependant aujourd'hui presque tout peut se connecter à votre réseau domestique, y compris vos smartphones, téléviseurs, consoles de jeux, moniteurs de bébé, haut-parleurs, ou peut-être même votre voiture. Une fois que vous avez identifié tous les périphériques de votre réseau domestique, assurez-vous que chacun d'entre eux est sécurisé. Le meilleur moyen de le faire est de vous assurer que leurs mises à jour automatiques sont activées dans la mesure du possible. Les cyberattaquants trouvent constamment de nouvelles faiblesses dans différents appareils et systèmes d'exploitation. En activant les mises à jour automatiques, votre ordinateur et vos appareils exécutent toujours les logiciels les plus récents, ce qui les rend beaucoup plus difficiles à pirater.

Mots de passe

L'étape suivante consiste à utiliser un mot de passe fort et unique pour chacun de vos appareils et comptes en ligne. Les mots clés ici sont forts et uniques. Fatigué des mots de passe complexes qui sont difficiles à retenir et difficiles à taper? Nous aussi. Utilisez une phrase secrète à la place. C'est un type de mot de passe qui utilise une série de mots faciles à retenir, comme «Où est mon café?» Ou «Soleil-beignets-heureux-plage». Plus votre phrase de passe est longue, plus elle est forte. Un mot de passe unique signifie utiliser un mot de passe différent pour chaque appareil et compte en ligne. De cette façon, si un mot de passe est compromis, tous vos autres comptes et appareils sont toujours en sécurité. Vous ne pouvez pas vous souvenir de tous ces mots de passe forts et uniques? Pas d'inquiétudes, nous non plus. C'est pourquoi

Créer une maison Cyber-sécurisée

nous vous recommandons d'utiliser un gestionnaire de mots de passe, qui est un programme de sécurité spécial qui stocke en toute sécurité tous vos mots de passe dans un coffre-fort virtuel chiffré.

Enfin, activez la validation en deux étapes dès qu'elle est disponible, en particulier pour vos comptes en ligne. La vérification en deux étapes est beaucoup plus forte. Elle utilise en effet votre mot de passe, mais ajoute également une seconde étape, comme un code envoyé à votre smartphone ou une application sur votre smartphone qui génère le code pour vous. La vérification en deux étapes est probablement la seule et unique mesure que vous pouvez prendre en considération pour vous protéger en ligne et c'est beaucoup plus facile que vous ne le pensez.

Sauvegardes

Parfois, peu importe si vous vous montrez prudent, vous pouvez être piraté. Si tel est le cas, la seule façon de récupérer vos informations personnelles est souvent de les restaurer à partir de la sauvegarde. Assurez-vous d'effectuer des sauvegardes régulières de toutes les informations importantes et vérifiez que vous pouvez les restaurer. La plupart des appareils mobiles prennent en charge les sauvegardes automatiques sur le Cloud. Pour la plupart des ordinateurs, vous devrez peut-être acheter un logiciel ou un service de sauvegarde, qui est relativement bon marché et simple à utiliser.

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

Phrases de passe :	https://securingthehuman.sans.org/ouch/2017#april2017
Gestionnaires de mots de passe :	https://securingthehuman.sans.org/ouch/2017#september2017
L'authentification à deux facteurs :	https://securingthehuman.sans.org/ouch/2017#december2017
Sauvegardes :	https://securingthehuman.sans.org/ouch/2017#august2017

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