OUCH! | Août 2018

OUCH!

SANS SECURITY AWARENESS

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

Appareils domestiques intelligents

Quels sont les appareils domestiques intelligents?

Traditionnellement, seuls quelques-uns de vos appareils à la maison peuvent se connecter à Internet, comme votre ordinateur portable, votre smartphone ou votre console de jeu. Cependant, aujourd'hui, de plus en plus d'appareils se connectent à Internet, de vos ampoules et haut-parleurs à votre téléviseur, le système de verrouillage de votre porte ou même votre voiture. Il est fort probable que bientôt, presque tous les appareils de votre maison pourraient être connectés à Internet. Ces appareils connectés sont souvent appelés Internet des Objets (Internet of Things - IoT) ou appareils domestiques intelligents (Smart Home). Bien que ces appareils connectés apportent beaucoup de confort, ils présentent également des dangers importants.

Quel est le problème?

Plus le nombre d'appareils connectés au réseau de votre domicile est élevé, plus des erreurs sont susceptibles de se produire. Les pirates peuvent programmer vos appareils pour attaquer les autres, les fournisseurs peuvent collecter des informations détaillées sur vos activités, ou vos appareils peuvent être infectés et vous bloquer. La plupart des entreprises fabriquant ces appareils n'ont aucune expérience de la cybersécurité et considèrent la sécurité uniquement comme un coût. Par conséquent, la plupart des périphériques que vous achetez ne sont pas protégés ou ne comportent aucune sécurité. Par exemple, certains périphériques ont des mots de passe par défaut qui sont bien connus ou que vous ne pouvez pas mettre à jour ou configurer.

Comment puis-je me protéger?

Alors que pouvez-vous faire ? Nous voulons absolument que vous tiriez parti des périphériques connectés, en toute sécurité. Ces dispositifs peuvent fournir des fonctionnalités formidables qui rendent votre vie plus simple. En outre, à mesure que la technologie se développe, vous n'avez peut-être pas d'autre choix que d'utiliser des appareils intelligents. Voici les étapes clés que vous pouvez suivre pour vous protéger.

Connectez uniquement ce dont vous avez besoin : le moyen le plus simple de sécuriser un périphérique est de ne pas le connecter à Internet. Si vous n'avez pas besoin que votre appareil soit en ligne, ne le connectez pas à votre réseau Wi-Fi. Avez-vous vraiment besoin que votre grille-pain vous envoie des notifications sur votre téléphone?

Sachez ce que vous avez connecté : quels appareils avez-vous connectés à votre réseau domestique ? Vous n'êtes pas sûr ou vous ne vous souvenez pas ? Éteignez votre réseau sans fil et voyez ce qui ne fonctionne plus. Il peut ne pas tout capter mais vous serez surpris du nombre d'appareils que vous avez oublié.

Restez à jour : tout comme votre ordinateur et vos appareils mobiles, il est essentiel de garder tous vos appareils à jour. Si votre appareil a la possibilité de se mettre à jour automatiquement, activez-le.

Mots de passe : remplacez les mots de passe de vos appareils par un mot de passe complexe unique et robuste. Vous n'aurez probablement plus qu'à les entrer une seule fois. Vous ne vous souvenez pas de toutes vos phrases secrètes ? Ne vous inquiétez pas, nous non plus. Envisagez d'utiliser un gestionnaire de mot de passe pour les stocker en toute sécurité.

Options de confidentialité : si votre appareil vous permet de configurer des options de confidentialité, limitez la quantité d'informations qu'il recueille ou partage. Une option consiste à désactiver simplement toutes les capacités de partage d'informations.

Vendeur : Achetez vos appareils auprès d'une entreprise que vous connaissez et en qui vous avez confiance. Recherchez les produits qui prennent en charge la sécurité, vous permettant d'activer la mise à jour automatique, de modifier le mot de passe par défaut et de modifier les paramètres de confidentialité.

Toujours à l'écoute : Si un appareil peut prendre vos commandes vocales, soyez conscient qu'il écoute en permanence. Par exemple, vos appareils Alexa et Google Home peuvent enregistrer des conversations sensibles. Considérez cela lorsque vous déterminez où placer les appareils dans votre maison et examinez les options de confidentialité.

Réseau invité : Envisagez de placer vos appareils domestiques intelligents sur un réseau Wi-Fi «invité» distinct plutôt que sur le réseau Wi-Fi principal que vous utilisez pour vos ordinateurs et appareils mobiles. De cette façon, si un appareil intelligent est infecté, vos ordinateurs ou appareils mobiles sur votre réseau principal restent en sécurité.

Il n'y a aucune raison d'avoir peur des nouvelles technologies : il suffit de comprendre le risque qu'elles représentent. En suivant ces quelques étapes simples, vous pourrez créer une maison intelligente bien plus sécurisée.

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.

Editeur invité

Robert M. Lee *(@RobertMLee) est un instructeur certifié SANS et auteur de FOR578 - Cyber Threat Intelligence et ICS515 - ICS Active Defense and Incident Response. Robert est également le PDG et le fondateur de la firme de cybersécurité industrielle Dragos.*

Sources

Phrases de passe :	https://www.sans.org/u/GEB
Gestionnaires de mots de passe :	https://www.sans.org/u/GEG
Sécuriser votre réseau domestique :	https://www.sans.org/u/GEL

OUCH! est publiée par le programme SANS (Security Awareness) et est distribuée sous la licence « Creative Commons BY-NC-ND 4.0 ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subie aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter www.sans.org/security-awareness/ouch-newsletter.
Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet