SANS SECURITY AWARENESS
Pélissier & Partners
Explorateurs de connaissances

OUCH! | Décembre 2017

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

OUCH!

Dans ce numéro...

Verrouillez votre connexion

Vue d'ensemble

Editeur invité

Tiffany Schoenike est la directrice des campagnes et des initiatives de la National Cyber Security Alliance (**@staysafeonline**). En 2016, Mme Schoenike a travaillé avec la Maison Blanche, le gouvernement et l'industrie pour développer et lancer Lock Down Your Login (Verrouiller votre connexion), une campagne STOP. THINK. CONNECT.™ relative à l'authentification à deux facteurs.

Le processus d'authentification, ou la preuve de qui vous êtes, est la clé pour protéger vos informations telles que vos e-mails, les médias sociaux ou vos comptes bancaires en ligne. Vous ne le savez peut-être pas, mais il existe trois façons de prouver qui vous êtes. Ce que vous savez - comme un mot de passe, ce que vous avez - comme votre permis de conduire, et ce que vous êtes - comme votre empreinte digitale. Chacune de ces méthodes présente des avantages et des inconvénients. La méthode d'authentification la plus courante est celle des mots de passe, quelque chose que vous connaissez. Malheureusement, l'utilisation de mots de passe se révèle de plus en plus insécurisée. Dans ce numéro, nous vous apprenons comment vous protéger et à verrouiller votre connexion avec quelque chose de bien plus fiable que des mots de passe, c'est ce qu'on appelle l'authentification à deux facteurs.

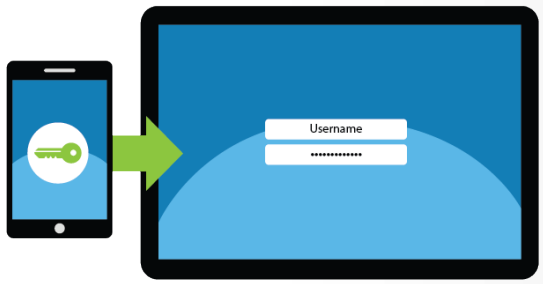
Les mots de passe ne sont plus suffisants

Les mots de passe prouvent qui vous êtes et sont basés sur quelque chose que vous connaissez. Mais si quelqu'un peut deviner ou avoir accès à votre mot de passe, il peut prétendre être vous et accéder à toutes vos informations. Les mots de passe compromis sont devenus l'une des principales causes des comptes piratés. C'est pourquoi vous apprendrez à utiliser des mots de passe difficiles à deviner pour les autres, un mot de passe différent pour chaque compte et à ne jamais partager vos mots de passe avec d'autres. Bien que ce conseil reste valable, les mots de passe ne sont plus aussi efficaces. Heureusement, il existe un moyen simple et rapide de vous contrôler et de protéger vos informations personnelles: l'authentification à deux facteurs.

Verrouillez votre connexion

Qu'est-ce que l'authentification à deux facteurs?

L'authentification à deux facteurs (également appelée vérification en deux étapes, authentification multi-facteurs ou 2FA) est beaucoup plus efficace que la simple utilisation de mots de passe. Elle fonctionne en exigeant non pas une, mais deux méthodes différentes pour prouver que vous êtes ce que vous dites être. Votre carte bancaire est un bon exemple. Lorsque vous retirez de l'argent d'un distributeur automatique de billets, vous utilisez une authentification à deux facteurs. Pour accéder à votre argent, vous avez besoin de deux choses, votre carte bancaire (quelque chose que vous avez) et votre code PIN (quelque chose que vous connaissez). Si votre carte bancaire est perdue ou volée, les autres ne peuvent pas retirer votre argent sans connaître votre code PIN. Un voleur doit avoir à la fois votre carte bancaire et votre code PIN pour effectuer un retrait. L'authentification à deux facteurs utilise le même concept.



Verrouillez votre connexion en utilisant l'authentification à deux facteurs dans la mesure du possible, c'est l'une des mesures les plus fortes que vous pouvez utiliser pour vous protéger en ligne.

Comment fonctionne l'authentification à deux facteurs?

L'authentification à deux facteurs est largement disponible sur la plupart des principaux sites bancaires, e-mails, réseaux sociaux et autres sites. En outre, la plupart de ces sites proposent des instructions simples, étape par étape, pour activer l'authentification à deux facteurs (pour plus d'informations, voir la section sources à la fin de ce numéro). Une fois que vous avez activé l'authentification à deux facteurs, vous pouvez vous attendre à ce que cela fonctionne comme suit. Premièrement, vous vous connectez à votre compte en utilisant votre nom d'utilisateur et votre mot de passe, comme vous l'avez toujours fait. C'est le premier des deux facteurs - quelque chose que vous connaissez. Ensuite, vous recevrez un code unique, souvent par SMS sur votre smartphone. Vous entrez ensuite ce code dans l'écran de connexion. C'est le deuxième des deux facteurs - vous devez avoir votre téléphone pour recevoir ce code. Maintenant, votre compte est vraiment verrouillé. Même si un cybercriminel vole votre mot de passe, il ne peut accéder à votre compte à moins qu'il ne possède votre téléphone.

Verrouillez votre connexion

Au lieu de recevoir le code unique via la messagerie texte, vous pouvez installer une application d'authentification spéciale sur votre smartphone. Cette application mobile génère un code unique pour vous chaque fois que vous souhaitez vous connecter. L'avantage d'utiliser une application mobile est qu'elle est encore plus sécurisée puisque le code est généré via l'application et n'est pas envoyé via la messagerie texte. En outre, il est plus pratique car vous n'avez pas besoin d'être connecté à un service téléphonique pour recevoir votre code unique. L'application génère constamment de nouveaux codes que vous pouvez utiliser pour vous connecter à votre compte.

Bien que l'authentification à deux facteurs puisse sembler représenter plus de travail au début, vos informations personnelles seront beaucoup plus sécurisées. N'attendez pas que vos comptes aient été piratés, verrouillez vos identifiants en activant l'authentification à deux facteurs sur vos comptes clés tels que les e-mails, les services bancaires ou les réseaux sociaux et bénéficiez d'une plus grande tranquillité d'esprit.

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
Sites proposant l'authentification à deux facteurs :	https://twofactorauth.org
Stop|Think|Connect :	https://www.lockdownyourlogin.org
La validation en deux étapes de Google :	http://www.google.com/landing/2step/

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

