OUCH! | Septembre 2015

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

OUCH!

Dans ce numéro...

La vérification en deux étapes

Vue d'ensemble

Le processus pour prouver qui vous êtes (appelée authentification) est la clé de protection de vos informations. L'authentification forte tente de s'assurer que vous pouvez accéder à vos informations, telles que votre e-mail, vos photos ou vos comptes bancaires. Il y'a trois façons différentes pour confirmer qui vous êtes; ce que vous savez - comme un mot de passe, ce que vous avez - comme un permis de conduire, et ce que vous êtes - comme votre empreinte digitale. Chacun de ces procédés présente des avantages et des inconvénients. La méthode la plus courante est les mots de passe soit quelque chose que vous connaissez. Dans ce numéro, nous allons vous apprendre à vous protéger avec la vérification en deux étapes, méthode beaucoup plus sécurisée que les mots de passe et pourtant très simple à utiliser. Pour mieux comprendre la vérification en deux étapes, nous devons commencer par les mots de passe.

Editeur invité

Keith Palmgren a plus de 30 ans d'expérience dans la sécurité de l'information. Il est un instructeur certifié au SANS Institute et auteur de SANS SEC301, une introduction de cinq jours au cours de sécurité de l'information. Lorsqu'il n'enseigne pas, Keith se concentre sur des projets de conseil et d'écriture. Vous pouvez suivre Keith sur **@kpalmgren**.

Mots de passe

Les mots de passe prouvant qui vous êtes, sont basés sur quelque chose que vous savez. Le danger avec les mots de passe est qu'ils sont un point de défaillance unique. En effet, si quelqu'un peut deviner ou accéder à votre mot de passe, il peut alors se faire passer pour vous et accéder à toutes vos informations. Ceci est la raison pour laquelle on vous enseigne des mesures pour protéger votre mot de passe, comme l'utilisation de mots de passe forts qui sont difficiles à deviner pour autrui, utiliser un mot de passe différent pour chaque compte ou encore ne jamais partager vos mots de passe avec les autres. Bien que ce conseil reste valable, les mots de passe vont souvent au-delà de leur utilité, ils ne sont plus efficaces dans le contexte actuel. Avec les technologies récentes, il est devenu beaucoup trop facile pour les cybers attaquants de compromettre les mots de passe. Nous avons besoin d'une solution facile à utiliser, encore plus sécurisée pour l'authentification forte. Heureusement, une telle option est maintenant couramment disponible : c'est ce que l'on appelle la vérification en deux étapes.

La vérification en deux étapes

La vérification en deux étapes (parfois appelée authentification à deux facteurs ou 2FA) est une solution plus sécurisée que les mots de passe. Elle fonctionne en exigeant non pas une mais deux méthodes différentes pour vous authentifier. Un exemple est votre carte de guichet automatique. Lorsque vous retirez de l'argent d'un guichet automatique, vous utilisez en fait une forme de vérification en deux étapes. Pour accéder à votre argent, vous avez besoin de deux choses, votre carte de guichet

La vérification en deux étapes

automatique (quelque chose que vous avez) et votre NIP (quelque chose que vous savez). Si vous perdez votre carte de guichet automatique, votre argent est toujours en sécurité. En effet, toute personne qui trouve votre carte ne peut pas retirer votre argent car elles ne connaissent pas votre code PIN (à moins que vous ayez écrit votre NIP sur votre carte, ce qui est une très mauvaise idée). C'est la même chose si elles ont seulement votre code PIN et pas votre carte. Un attaquant doit disposer des deux pour pouvoir compromettre votre compte bancaire. Voilà ce qui fait que la vérification en deux étapes est beaucoup plus sécurisée : vous avez deux couches de sécurité.

Utilisez la vérification en deux étapes chaque fois que possible, il s'agit de l'une des mesures les plus fortes que vous pouvez prendre en considération pour protéger vos informations.

Utiliser la vérification en deux étapes

La vérification en deux étapes est quelque chose que vous avez configuré individuellement pour chacun de vos comptes. Heureusement, de nombreux services en ligne l'offrent. Un des chefs de file dans la vérification en deux étapes est Google. Les comptes Google sont une cible de choix pour les pirates informatiques car ils offrent une grande variété de services en ligne gratuits pour des millions de personnes dans le monde. En tant que tel, Google se devait de fournir une authentification forte et a d'ailleurs été l'une des premières organisations à déployer la vérification en deux étapes pour la plupart de ses services en ligne. Si vous comprenez comment les deux étapes de vérification de Google fonctionnent, vous comprendrez également comment la vérification en deux étapes fonctionne pour la plupart des autres sites tels que Twitter, Facebook, Apple, Instagram et de nombreuses banques.

Tout d'abord, vous devez activer la vérification en deux étapes sur votre compte Google et inscrire votre numéro de téléphone mobile. Une fois cette étape terminée, la vérification en deux étapes fonctionne comme suit. Vous vous connectez à votre compte tout comme avant avec votre nom d'utilisateur et votre mot de passe. Ceci est le premier des deux facteurs - quelque chose que vous savez. Google envoie ensuite un message texte sur votre téléphone mobile contenant un code unique, spécifiquement une chaîne de six numéros. Tout comme votre mot de passe, vous entrez alors ces six numéros sur le site. Ceci est le second des deux facteurs. Donc, pour vous connectez avec succès à votre compte, vous devez à la fois connaître votre mot de passe et avoir votre téléphone mobile pour recevoir les codes uniques. Même si un attaquant détient votre mot de passe, il ne pourra pas accéder à votre compte Google à moins qu'il ait également votre téléphone. Pour assurer que votre compte est vraiment sécurisé, Google vous enverra un nouveau code unique à chaque fois que vous vous connecterez.

Il existe une autre solution pour la vérification en deux étapes avec Google et de nombreux autres sites. Au lieu de recevoir le code unique par messagerie texte SMS, vous pouvez installer une application d'authentification sur votre smartphone. L'application génère le code unique chaque fois que vous voulez vous connecter. L'avantage avec l'aide d'une application mobile est que vous

La vérification en deux étapes

ne devez pas être connecté à un service de téléphone pour recevoir votre code unique, votre téléphone le génère pour vous. De plus, le code est généré localement sur votre téléphone et ne vous est pas envoyé, il ne peut par conséquent pas être intercepté.

Rappelez-vous, la vérification en deux étapes n'est pas activée par défaut, vous devez l'activer vous-même. Bien que la vérification en deux étapes peut sembler représenter plus de travail au début, nous vous recommandons fortement de l'utiliser chaque fois que possible, en particulier pour les services essentiels tels que vos comptes de messagerie, les services bancaires en ligne ou le stockage de vos fichiers en ligne. La vérification en deux étapes va beaucoup plus loin pour protéger vos informations que de simples mots de passe.

Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

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/

Sources

Phrases de passe :	http://www.securingthehuman.org/ouch/2015#april2015
Vérification en deux étapes :	https://twofactorauth.org
Utilisation du Cloud en toute sécurité :	http://stopthinkconnect.org/2stepsahead
Chiffrement :	http://www.google.com/landing/2step/
Conseil du jour :	http://www.sans.org/tip_of_the_day.php

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