Choisir de bons mots de passe - Guide de l'utilisateur

Ce document présente un guide en langage simple pour aider les utilisateurs à comprendre comment les mots de passe sont compromis et comment choisir des mots de passe sécurisés.

Le défi de la gestion des mots de passe

Les mots de passe sont utilisés pour protéger divers systèmes et services - courrier électronique, connexions au réseau et aux ordinateurs, applications et plus encore. Les utilisateurs doivent choisir un mot de passe lors de la configuration d'un nouveau compte et, dans de nombreux cas, changer périodiquement ce mot de passe.

Pourquoi changer les mots de passe?

La chose la plus simple à faire est d'avoir un seul mot de passe sur tous les systèmes et ne jamais le changer. Le problème avec cette stratégie est que si l'un de ces systèmes est compromis, alors les mots de passe sur ce système peuvent être révélés. Un mot de passe compromis sur un système peut être utilisé pour se connecter à un autre système où le même utilisateur possède un compte.

Pour atténuer ce risque, il est raisonnable de changer les mots de passe périodiquement et d'utiliser des mots de passe différents sur différents systèmes. Comme il est difficile de se rappeler beaucoup de mots de passe différents, un compromis raisonnable est d'utiliser quelques mots de passe - par exemple, un pour les services aux consommateurs comme Facebook ou Google, Un autre pour les sites Web de commerce électronique; Un autre pour la banque personnelle et un autre pour le travail.

Choisir des mots de passe difficiles à deviner

Il est tentant de choisir quelque chose de trivial et facile à retenir, comme l'orthographe de votre nom d'utilisateur vers l'arrière, le nom d'un enfant ou un mot de dictionnaire. Le problème est, plus le mot de passe est simple, plus il sera facile pour un attaquant de deviner.

Les attaquants ont souvent accès aux systèmes en devinant ou en compromettant un ID de connexion et un mot de passe. Après avoir obtenu ces informations d'identification, un attaquant peut alors emprunter l'identité d'un utilisateur valide.

Si l'attaquant vous connaît, il peut essayer des combinaisons de mots de passe liées à votre famille, à vos intérêts ou à votre historique. S'ils ont un accès physique à votre bureau, votre PC ou votre téléphone, vos chances d'accéder à vos comptes sont encore plus importantes, car votre mot de passe peut être écrit ou stocké électroniquement, en texte clair, sur l'un d'eux.

Les attaquants utilisent un logiciel facilement disponible pour essayer rapidement des mots de passe plausibles, basés sur les mots du dictionnaire et les noms d'utilisateur, jusqu'à ce qu'ils aient frappé un mot de passe valide. Si un attaquant peut obtenir une copie d'une base de données de mots de passe cryptés, il peut tester des milliards de mots de passe par seconde, pour vérifier si certains sont corrects. À ce rythme, un attaquant peut deviner plusieurs mots de passe en quelques heures.

Plus le mot de passe est court et plus prévisible, plus vite on peut le deviner. Les mots du dictionnaire orthographiés vers l'arrière, réarrangés ou avec des chiffres ajoutés sont dangereux. Les substitutions simples, telles que le remplacement de la lettre l ou i par le chiffre 1, sont également dangereuses, car le logiciel de détection de mot de passe les essayera.

Voici quelques exemples de mauvais mots de passe:

- mydog2
- bijoux
- Yromem (méLa solution la plus sûre pour choisir de bons mots de passe est d'utiliser un mot de passe aléatoire ou apparemment aléatoire qui:

- Est au moins 8 caractères.
- Contient un mélange de lettres majuscules et minuscules.
- Comprend des chiffres et des signes de ponctuation.
- N'est pas basé sur des renseignements personnels.
- N'est pas basé sur un mot du dictionnaire.

Voici quelques exemples de mots de passe forts:

- De2#vuX
- 5sd$oiP
- :er89TI:

Écriture de mots de passe

Si vous avez trop de mots de passe, il est tentant de les écrire - après tout, pouvez-vous vraiment se rappeler 10 mots de passe différents, qui changent à des moments différents, dont certains sont rarement utilisés?

Écriture de mots de passe est une grave violation de la sécurité, car cela signifie que toute personne qui peut physiquement obtenir le morceau de papier, la note collante ou le téléphone qui contient le mot de passe, peut également se connecter à des systèmes avec vos comptes. Un vendeur invité devrait-il vraiment être en mesure de signer dans la demande de financement? Le concierge doit-il pouvoir lire votre courrier électronique?

Une meilleure solution est de créer un mot de passe unique et fort et de l'appliquer à tous vos comptes de connexion. Un mot de passe est plus facile à retenir et est plus sécurisé qu'une note écrite.

Réutilisation des mots de passe

Une autre tentation, lorsque l'imagination échoue, est de réutiliser les anciennes valeurs de mot de passe quand vient le temps de changer votre mot de passe. C'est aussi un problème de sécurité, car le changement d'un mot de passe régulier consiste à limiter le temps dont dispose un attaquant pour détruire votre mot de passe. Si un ancien mot de passe est réutilisé, les attaquants auront plus de temps pour les deviner. Si l'ancien mot de passe était déjà compromis, le nouveau compromettra votre sécurité à nouveau.

Ceci est la traduction Google du texte original des deux pages suivantes

Choosing Good Passwords -- A User Guide

This document presents a plain-language guide to help users understand how passwords are compromised and how to choose secure passwords.

The password management challenge

Passwords are used to protect various systems and services -- e-mail, PC and network logins, applications and more. Users must choose a password when setting up a new account and in many cases must periodically change that password.

Why change passwords?

The simplest thing to do is to have just one password on all systems and never change it. The problem with this strategy is that if any of those systems is compromised, then passwords on that system may be revealed. A password compromised on one system can be used to sign into another system where the same user has an account.

To mitigate this risk, it is reasonable to change passwords periodically and to use different passwords on different systems. Since it's hard to remember lots of different passwords, a reasonable compromise is to use just a few passwords -- for example, one for consumer services like Facebook or Google; another for e-Commerce web sites; another for personal banking and another for work.

Choosing hard to guess passwords

It's tempting to pick something trivial and easy to remember, like spelling your user name backwards, a child's name or a dictionary word. The problem is, the simpler the password, the easier it will be for an attacker to guess.

Attackers often gain access to systems by guessing or otherwise compromising a login ID and password. Having gained these credentials, an attacker can then impersonate a valid user.

If the attacker knows you, they can try password combinations related to your family, interests or history. If they have physical access to your desk, PC or phone, their chances of getting into your accounts are even greater, as your password may be written down or electronically stored, in plaintext, on one of these.

Attackers use readily available software to rapidly try plausible passwords, based on dictionary words and user names, until they hit on a valid password. If an attacker can get a copy of an encrypted password database, they can test billions of password guesses per second, to see if any are correct. At this pace, an attacker can guess many passwords in just a few hours.

The shorter and more predictable the password, the faster it can be guessed. Dictionary words spelled backwards, rearranged or with digits added are unsafe. Simple substitutions, such as replacing the letter l or i with the digit 1 are likewise unsafe, as password guessing software will try these.

Examples of bad passwords include:

- mydog2
- bi11smith
- yromem (memory backwards)

- win4me

The safest solution for choosing good passwords is to use a randomly generated or seemingly random password that:

- Is at least 8 characters long.
- Contains a mix of upper and lower case letters.
- Includes digits and punctuation marks.
- Is not based on any personal information.
- Is not based on any dictionary word.

Examples of strong passwords include:

- De2#vuX
- 5sd$oiP
- :er89TI:

Writing passwords

If you have too many passwords, it is tempting to write them down -- after all, can you really remember 10 different passwords, that change at different times, some of which are rarely used?

Writing down passwords is a serious breach of security, because it means that anyone who can physically get to the piece of paper, sticky note or phone that contains the password, can also log into systems with your accounts. Should a visiting vendor really be able to sign into the finance application? Should the janitor be able to read your e-mail?

A better solution is to create a single, strong password, and apply it to all of your login accounts. One password is easier to remember, and is more secure than a written note.

Reusing passwords

Another temptation, when imagination fails, is to reuse old password values when the time comes to change your password. This is also a security problem, since the whole point of a regular password change is to limit the time available to an attacker to crack your password. If an old password is reused, attackers will have more time to guess them. If the old password was already compromised, the new one will compromise your security again.

texte trouvé sur internet / 13 novembre 2016 / René Andrey

- -