

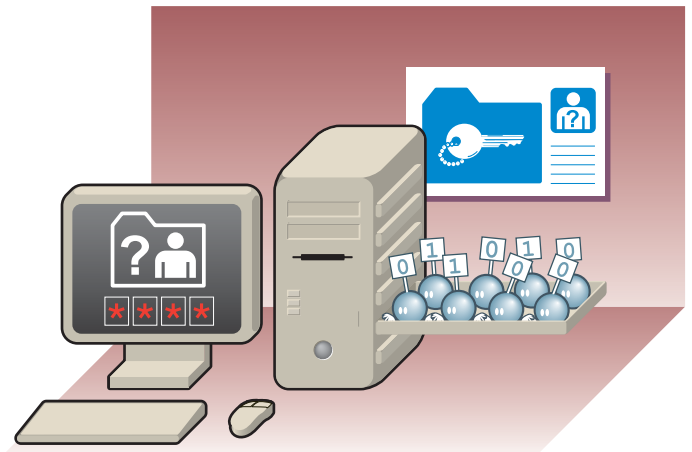
## Résumé

L'authentification par mot de passe (ou password en anglais) est une des plus anciennes techniques de sécurité. Elle est toujours fortement utilisée et compte comme sûre si quelques règles fondamentales sont respectées. Parmi les techniques d'authentification on peut aussi citer les certificats électroniques ou les empreintes digitales.

Lorsque vous allumez votre ordinateur, que vous souhaitez accéder à vos mails, que vous désirez vous rendre sur un site Internet privé ou consulter un fichier confidentiel on vous demande la plupart du temps de donner votre mot de passe, on vous demande en fait de vous authentifier avant de pouvoir accéder à une ressource.

## Table des matières

- 1 Qu'est-ce qu'un mot de passe? →
- 2 Quels sont les risques et les éviter? →
- 3 Comment choisir un bon mot de passe? →
- 4 Comment s'en souvenir? →
- 5 Au secours! J'ai perdu mon mot de passe →



Cette fiche est à mettre en étroite relation avec celle consacrée à l'authentification des utilisateurs sur un système informatique. Toutefois, ce document est plus précisément consacré aux mots de passe et aux aspects critiques les concernant.

## 1 C'est quoi?

Un mot de passe est une technique d'authentification qui n'est pas propre à l'informatique. Beaucoup de ces techniques sont basées sur un secret partagé entre celui qui souhaite s'authentifier (l'utilisateur) et celui qui demande l'authentification (la machine, le logiciel).

Ce secret est soit :

- Basé sur quelque chose que l'utilisateur possède (cartes, badges, documents...)
- Basé sur quelque chose que l'utilisateur est (techniques biométriques...)

→ Basé sur quelque chose que l'utilisateur connaît de lui seul (mots de passe...)

→ Basé sur la combinaison de ces techniques (cartes de crédit...)

Généralement le système qui demande l'authentification par mot de passe ne stocke pas le mot de passe en clair mais une forme dérivée grâce à des fonctions mathématiques très complexes (hash). Votre mot de passe et cette fonction hash permettent de vous authentifier et non votre mot de passe seul.

## 2 Quels sont les risques et comment les éviter?

### Prudence

Si quelqu'un découvre votre mot de passe, le principal risque est que cette personne usurpe votre identité. Elle peut se faire passer pour vous et par exemple lire et répondre à vos mails, utiliser votre GSM, virer tout votre argent sur un autre compte bancaire,

utiliser votre ordinateur pour accomplir des actes de piratage dont vous seriez responsable ou de vous surveiller voire espionner votre société. Ces opérations étant effectuées sous votre identité, il vous faudra après démontrer que vous n'êtes pas l'auteur de ces actes et cela est parfois impossible !

Si jamais vous pensez que quelqu'un d'autre connaît votre secret, prévenez immédiatement la personne compétente et responsable du système, par exemple votre administrateur système, votre banque ou votre fournisseur d'accès et changez immédiatement le mot de passe.

## → CONSEIL:

Composez vos identifiants à l'abri des regards indiscrets et évitez de les communiquer à quelqu'un d'autre. Méfiez-vous si quelqu'un prétend avoir besoin de votre mot de passe pour une tâche très importante comme par exemple l'ingénieur réseau. Une telle requête provient généralement d'une personne malveillante !

## 3

### Comment choisir un bon mot de passe ?

Les gens ont tendance à choisir toujours les mêmes mots de passe ou qui leur soient facile à se rappeler comme le nom de leurs enfants, de leur animal préféré, leur date de naissance ou leur surnom. Quelqu'un qui vous connaît un tant soit peu est donc capable de cracker votre mot de passe. Il faut donc choisir le mot de passe le plus arbitraire possible.

Hormis cette faille, il existe deux autres types d'attaque courante :

#### → Les attaques par dictionnaire

Les mots contenus dans un dictionnaire sont à proscrire et sont très vulnérables puisque issus d'un ensemble connu de tous. En résumé le pirate va essayer de casser votre code en testant tous les mots du dictionnaire (des outils informatiques très performants peuvent réaliser de telles attaques).

#### → Les attaques par force brute

Le pirate va essayer de casser votre code en testant toutes les possibilités inimaginables. Pour vous en prémunir choisissez un mot de passe d'au moins 8 caractères et composé de chiffres, de lettres et de symboles. Plus votre mot de passe sera long plus cela lui prendra du temps et sera hors de portée de sa machine.

→ Vous devez être capable de retenir vos mots de passe par cœur. Il existe d'ailleurs des logiciels spécialisés pour vous aider dans ce domaine. En effet, les systèmes d'authentification sont conçus de telle sorte qu'ils n'acceptent qu'un nombre limité de fausses entrées avant de bloquer définitivement ou temporairement l'accès au compte utilisateur en question.

## → CONSEIL:

Caractéristiques d'un bon mot de passe :

- Au minimum 8 caractères (le plus le mieux).
- Composé de chiffres, de lettres majuscules, de lettres minuscules et de symboles.
- Il ne doit pas être basé sur un mot du dictionnaire.
- Il ne doit pas reposer sur une information personnelle.
- Il doit être différent pour chaque application, fichier, système que vous utilisez.
- Il doit être arbitraire.
- Changez-les souvent, au strict minimum tous les semestres, selon leur utilité.

## 4

### Comment s'en souvenir ?

Évitez de noter vos mots de passe sur un post-it collé sur votre écran, caché en dessous de votre clavier ou dans votre portefeuille sous forme d'un numéro de téléphone. Les personnes mal intentionnées connaissent tous ces petits trucs et savent les déjouer. Votre meilleur atout c'est vous-même ! Et votre mémoire.

Dans le cas où vos mots de passe deviendraient trop nombreux, vous pouvez toujours utiliser un logiciel spécialisé dans le stockage des mots de passe (voir liens). C'est une bonne solution mais il vous faudra un mot de passe pour le faire fonctionner, donc choisissez-le bien sinon on pourrait découvrir l'ensemble de vos mots de passe.

## → CONSEIL:

Un bon moyen de se souvenir de ses identifiants est d'utiliser un moyen mnémotechnique comme par exemple « la phrase magique ». Composez une phrase avec des mots commençant par chacun des caractères de votre mot de passe.

« Il était une fois 3 petits cochons : Pim Pam Poum » donne le mot de passe (hautement sécurisé) Iéuf3pc:PPP.

5

## Au secours, j'ai perdu mon mot de passe !

Si vous avez oublié votre mot de passe, pas de panique ! Prévenez la personne compétente et responsable du système pour qu'elle vous en donne un nouveau immédiatement. S'il s'agit d'un mot de passe par défaut, personnalisez le tout de suite.

En ce qui concerne les authentications par Internet, il existe généralement un mécanisme de récupération. Il vous suffit de donner votre identité et un mail vous est envoyé contenant le mécanisme de récupération à l'adresse électronique fournie au moment de votre inscription. Détruisez ce mail une fois utilisé.