

Sécuriser son authentification : Gérer ses mots de passe

Définition d'un mot de passe "fort"

Lorsqu'un mot de passe apporte un niveau de sécurité suffisant, on parle de mot de passe fort. C'est à dire qu'il est difficile à découvrir par un attaquant dans un temps raisonnable, à l'aide d'outils automatisés de recherche qui mettent en oeuvre les différentes techniques d'attaque (attaques par dictionnaire, force brute, permutation, distribués, de proximité, etc...).

Exemple de mot de passe "fort"

Compte tenu des capacités techniques actuelles des équipements informatique, la taille d'un mot de passe est idéalement d'au moins 11 caractères en utilisant un large éventail de caractères (majuscules, minuscules, chiffres et caractères spéciaux).

Voici ci-dessous un exemple concret de mot de passe fort :

G&LmE1vB@2[✓]



Règles à appliquer pour créer un mot de passe "fort"

Pour créer un mot de passe fort, il est requis de suivre les règles suivants :

-  **Minimum 11 caractères.**
-  **Un Jeu de caractères variés** *(pas uniquement des lettres et des chiffres).*
-  **Sans référence à vos informations personnelles** *(nom, prénom, date de naissance, nom des enfants, de son animal de compagnie).*
-  **Bannir les mots du dictionnaire** *(rendre le mot de passe difficile à deviner).*
-  **Ne pas utiliser un mot de passe plusieurs fois** *(ex: un mot de passe par application).*



Sécuriser son authentification : Gérer ses mots de passe



Comment mémoriser des mots de passe ?

Vous vous demandez certainement comment retenir un mot de passe comme **"G&LmE1vB@2"** ?

Pour le retenir il sera pratiquement nécessaire de l'écrire quelque part. Mais **le noter serait une erreur** car cela représenterait un risque important en terme de divulgation.

Ainsi, voici quelques méthodes pour créer **un mot de passe qui soit à la fois "fort" et simple à retenir**.

Méthode 1 : *"Définir une phrase"*

Le principe de cette méthode est de **prendre plusieurs mots au hasard puis de les concaténer**.

Exemple : **"2Lunettes:5Crayons:1Chien"** ou encore **"1Clavier?travail.2fenetres.5arbre"**.

Ces mots facilement mémorisables sont difficilement trouvables par un individu malveillant.



Sécuriser son authentification : Gérer ses mots de passe

Méthode 2 : "Utiliser la phonétique"

Cette deuxième méthode consiste à utiliser la phonétique. C'est à dire retenir les sons de chaque syllabe pour fabriquer une phrase facile à retenir.

Exemple :

- *"J'ai acheté huit CD pour cent euros cet après-midi"* = **ght8CD%€7am.**
- *"Trois cadeaux à Noël"* = **3KDO@nowel**

Ces mots facilement mémorisables sont en revanche difficilement trouvables par un individu malveillant.

Méthode 3 : "Citation, phrase, ..."

Cette méthode consiste à retenir les premières lettres d'une phrase comme une citation, ou encore les paroles d'une chanson. Vous pouvez également rajouter des chiffres à la fin de la phrase pour obtenir 11 caractères.

Exemple :

- *"Un tiens vaut mieux que deux tu l'auras"* = **1Tvmq2tl@**
- *"Rien ne sert de courir, il faut partir à point"* = **Rns2clfp@p**



Sécuriser son authentification : Gérer ses mots de passe

Méthode 4 : *“Suite complexe plus un identifiant unique”*

Enfin, voici une dernière méthode intéressante pour créer et retenir plusieurs mots de passe complexes. Il faut ici créer une suite complexe avec des caractères variés et terminer (*ou commencer*) la suite par un identifiant uniquement de deux ou trois caractères. Par exemple les premières lettres (*ou dernières lettres*) du système, de l'application ou encore du site en question.

Exemple :

1. Création d'une suite complexe **“Ghk@IoP12”**.
2. Associer ensuite cette suite avec l'identifiant (ex: deux premières lettres) du système, de l'application ou du site.
3. Pour se connecter à Windows **“Ghk@IoP12Wi”** ou pour se connecter à son compte Google **“Ghk@IoP12Go”**.

Enfin, rien ne vous empêche de combiner plusieurs de ces quatre méthodes. Retenez que ces différents moyens mnémotechniques vous permettront de définir des mots de passe sécurisés et faciles à retenir.

[Générer un mot de passe fort depuis le site de la CNIL](#)



Sécuriser son authentification : Gérer ses mots de passe

Utiliser un “coffre fort” de mots de passe

Comme vous avez pu le constater la méthode de mémorisation que nous avons vu précédemment est extrêmement efficace. Cependant à l'usage cela n'est pas toujours simple et/ou pertinent. En effet, certains sites internet n'autorisent pas de caractères spéciaux ou n'autorisent que des chiffres.

Ainsi, une autre solution qui est peut-être la plus pratique est de **déléguer à un logiciel la mémorisation de son mot de passe**.

L'une des solutions les plus sécurisées pour ce type de besoin est la solution [KeePass](#). Ce logiciel recommandé par l'ANSSI et la CNIL permet de gérer tous vos mots de passe dans un coffre fort. Vous n'avez alors qu'à vous souvenir d'un seul mot de passe fort pour accéder à l'ensemble de vos mots de passe. De plus, cette solution permet de créer des mots de passe complexes très simplement.



Sécuriser son authentification : Gérer ses mots de passe

Autres solutions de coffre fort de mots de passe

Evidemment il existe bien d'autres solutions pour gérer ses mots de passe. Solutions qui permettent notamment de les gérer très simplement en les stocker sur un espace de type Cloud. Cependant, il faut ici bien avoir conscience qu'à la différence de KeePass nous délégons dans ce cas la gestion et le stockage de nos mots de passe à un prestataire.

Malgré tout ces services semblent également sécurisés et elles offrent il faut l'avouer une plus grande simplicité d'usages. A vous ici de faire le choix qui vous paraît le plus pertinent pour vous.

- [Lastpass](#)
- [1Password](#)
- [Dashlane](#)
- [BitWarden](#)

