



## PRISE EN MAIN DES MOTS DE PASSE

Entre les réseaux sociaux, les adresses mails, les comptes bancaires, les sites d'e-commerce, nous avons besoin d'un nombre croissant d'identifiants et de mots de passe. Voici donc un petit récapitulatif des erreurs à ne pas commettre de petites astuces pour générer et retenir ses différents mots de passe.

### Règles générales sur la création d'un mot de passe

- Un bon mot de passe doit contenir **au moins 12 caractères** dont 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- **Altern**er les lettres minuscules et majuscules.
- **Personne ne doit deviner** votre mot de passe à partir d'éléments connus de tous (chien, date de naissance, deuxième prénom).
- Utiliser un **mot de passe différent** pour chaque site internet.
- **Renouveler le plus fréquemment possible** son mot de passe, au moins tous les trois mois. Il n'est pas suffisant de simplement ajouter un chiffre à la fin.



### Les erreurs à éviter



- Des mots de passe trop simples : 123456, 123456789, qwerty, password, 111111...
- Des prénoms
- Des noms d'équipe sportive
- Des artistes ou musiciens
- Des personnalités fictives ou non
- Des informations connues par vos proches
- Utiliser le même mot de passe sur vos nombreux sites internet (messagerie, banque, achat en ligne, etc.)
- Conserver la liste de ses mots de passe sur un fichier texte, dans votre messagerie ou téléphone
- Communiquer ses mots de passe à un tiers

## Astuces pour générer ses mots de passe



- Choisir 5 mots au hasard pour en faire une phrase qui ne veut rien dire.
- Ajouter des chiffres, majuscules et caractères spéciaux à des endroits que vous pouvez retenir

L'agence Nationale de la sécurité des systèmes d'information donne deux bonnes idées pour trouver de bons mots de passe :

- La **méthode phonétique** : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am
- La **méthode des premières lettres** : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

## Vérifier la solidité de votre mot de passe

Certains services, comme Outlook.com, évaluent au fur et à mesure que vous le tapez le niveau de sécurité de votre mot de passe. Vous pouvez, si cette option n'existe pas, évaluer le degré de fiabilité de votre mot de passe grâce à un service comme Password Meter ([www.passwordmeter.com](http://www.passwordmeter.com)) ou un logiciel comme Password Pond (gratuit, en anglais).

Il est vraiment important de sécuriser le mot de passe de sa boîte mail. Votre boîte mail est en effet liée à une grande partie de vos comptes. Si sa sécurité était compromise, un pirate n'aurait aucun mal à récupérer vos autres mots de passe par ce biais.

## Comment retenir les différents mots de passe

Avec autant de comptes, retenir tous ses mots de passe est quasiment impossible. Du coup on change à nouveau, on opte pour quelque chose de plus simple, on refait les mêmes erreurs et on revient au point de départ.

Certains notent les différents mots de passe sur des supports papier mais les calepins, cahiers, bouts de papiers ne sont pas sécurisés.

Ils ont ainsi créé ce que l'on appelle des gestionnaires de mots de passe.

Ces logiciels pour ordinateurs, téléphones et tablettes sont en fait des coffres forts numériques. Ils sont ultra-sécurisés et stockent tous vos mots de passe.

Ce coffre va retenir tous vos mots de passe à votre place. Vous n'aurez qu'un seul et unique mot de passe à retenir pour sécuriser le coffre-fort. Ce mot de passe doit être ultra-sécurisé et reprendre les règles citées plus haut.

Voici trois logiciels de gestionnaires de mots de passe : Dashlane, KeePass ou encore 1Password.

## Bibliothèque Pierre GOY

4 place du Clos Fleury, 74100 ANNEMASSE - Tél. 04 50 95 89 09

[bibliotheque.annemasse@annemasse.fr](mailto:bibliotheque.annemasse@annemasse.fr)

[www.bibliotheques-intermede.fr](http://www.bibliotheques-intermede.fr)

[facebook.com/bibliothequesintermede](https://facebook.com/bibliothequesintermede)