Mot de passe

Quelles sont les bonnes pratiques générales à appliquer ?

1. Utiliser un mot de passe différent pour chaque accès

2. Choisir un mot de passe robuste

3. Changer votre mot de passe au moindre doute

4. Garder ses mots de passe pour soi

5. N'utilisez pas vos mots de passe sur un ordinateur partagé

6. Changez les mots de passe par défaut des services que vous utilisez

7. Choisissez un mot de passe particulièrement complexe pour votre boîte de messagerie

Mot de passe : création

Comment créer un mot de passe sécurisé ?

1. Créer soi-même son mot de passe

7 techniques pour créer le mot de passe parfait

- **La technique de la forme géométrique**
- **La technique du décalage**
- **La technique des acronymes**
- **La technique des néologismes**
- **La technique du cyber-langage**
- **La technique du ‘consonnes only’**
- **La technique du codage de geek**

2. Utiliser un générateur de mots de passe

https://www.motdepasse.xyz/

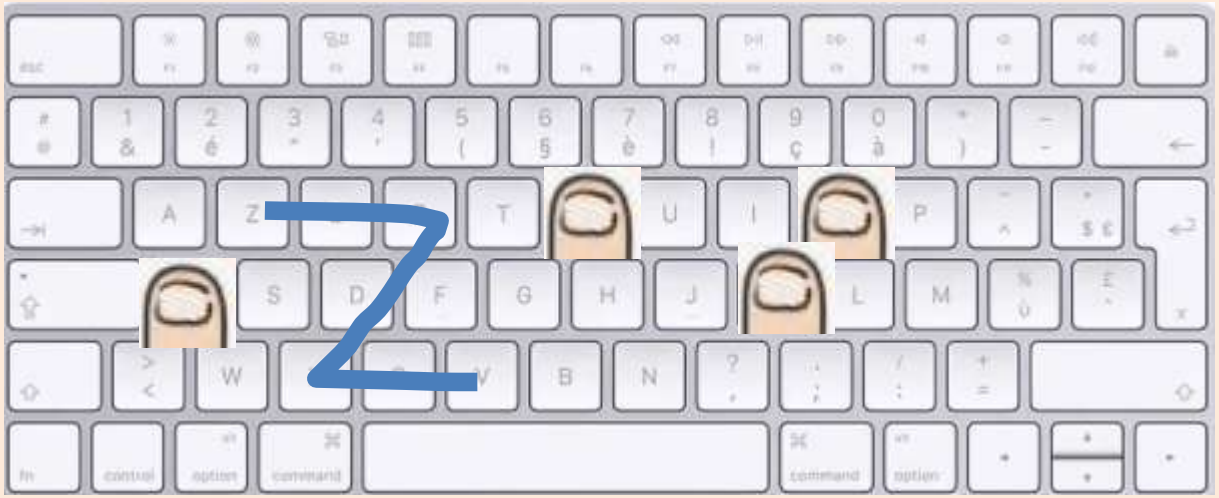
http://www.generateur-motdepasse.com/

https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

Mot de passe : création

- **La technique de la forme géométrique**

zerdxcv



- **La technique du décalage**

plus

- **La technique des acronymes**

Cecmepb

Ce club me plaint bien

- **La technique des néologismes**

Tasse et statue deviennent **tasstatue**.

- **La technique du cyber-langage**

Je vais prendre le plat du jour :**jvéprendrelePDJ**

- **La technique du ‘consonnes only’**

jvsprndrlpltdjr

- **La technique du codage de geek**

Maxime deviendra **M4x1m3**.

Mot de passe : création

Top 10 dans le monde :

123456
123456789
1234
qwerty
Password
111111
123123

Temps pour cracker un mot de passe

moulinet → 13 mins

Moulinet → 2 jours

Moulin3t → 10 jours

Moulin3t# → 12 ans

Moulin3t@Paulo → 32 millairds d'années

Moulin3t_Fil0che% → 14 quadrillons d'années

quadrillon= 1 000 000 000 000 000 000 000 000

Mot de passe : Gestionnaire de mots de passe

À quoi sert un gestionnaire de mots de passe ?

Une fois que vous avez défini vos différents mots de passe, il faut tous les mémoriser, ce qui n'est pas toujours simple. En effet, qui n'a jamais douté ou oublié un mot de passe ?
Pour ne pas avoir à demander un nouveau mot de passe à chaque oubli, **le gestionnaire de mots de passe** se charge de tout mémoriser pour vous. Très simple d'utilisation, il vous permet d'avoir accès à tout moment à l'ensemble de vos codes d'accès.

Nous vous recommandons fortement d'utiliser l'outil KeePass, seul gestionnaire français gratuit qui soit certifié par l'ANSSI.

Mot de passe : le gestionnaire KeePass

Keepass : chiffrez vos mots de passe sur Windows et Mac

KeePass : retenez un seul mot de passe et chiffrez tous les autres

Un gestionnaire de mot de passe simple et gratuit

Son principe est très simple : **KeePass sauvegarde tous vos mots de passe** dans une base de données qui lui est propre et qui est en réalité un fichier chiffré (« crypté »).

Un gestionnaire de mot de passe fiable et sécurisé

Vous aurez ainsi le choix entre **deux algorithmes de chiffrement** pour :

- une sécurisation par chiffrement **AES** (clé de 256 bits)
- une sécurisation par chiffrement **TwoFish** (clé de 256 bits + blocs de 128 bits)

Gérez vos mots de passe aussi sur mobile

La base de données contenant vos mots de passe chiffrés (ou chiffrés si l'on veut utiliser le terme correct) peut être **synchronisée à distance**.
Avec **l'application KeePass** installée sur votre smartphone vous pourrez être synchronisé depuis un site distant

Mot de passe : le gestionnaire KeePass

Une interface en glisser/déposer très facile d'utilisation

Encore plus simple avec la saisie automatique de mot de passe

Si vous désirez **gagner encore plus de temps**, vous pouvez dans KeePass renseigner l'identifiant et le mot de passe à utiliser pour une application ou pour un site (grâce à son URL) afin que celui-ci les mettent **automatiquement** à chaque lancement de l'application ou du site internet.

La meilleure option de KeePass selon nous

Une des failles majeures que l'on retrouve dans les gestionnaires de mots de passe est la gestion du presse papier lorsqu'un mot de passe est copié/collé.
KeePass permet alors de chiffrer les mots de passe en mémoire vive de votre ordinateur (et au passage de remplacer les caractères visibles par des astérisques).
Mais cela n'étant hélas pas suffisant pour garantir une sécurité optimale, **KeePass ne conserve en mémoire dans le presse papier que 12 secondes maximum un mot de passe copié/collé**.

Mot de passe : le gestionnaire KeePass

Les plugins de KeePass

• **l'enregistrement d'une sauvegarde de votre base de données** à chaque fois que celle-ci est mise à jour par de nouvelles entrées.
• l'utilisation de KeePass sur les **trois principaux navigateurs** que le grand public utilise avec **Chrome, Firefox et Internet Explorer**.
• l'utilisation de KeePass sur son **smartphone, sa tablette et ses ordinateurs** en les synchronisant sur un **cloud** contenant votre base de données.
• **l'importation et l'exportation** encore plus facile de vos données vers d'autres logiciels qui sont des gestionnaires de mot de passe concurrents à KeePass.
• l'utilisation d'une **protection par certificat** plutôt que par mot de passe permettant ainsi d'ajouter une sécurisation supplémentaire.
• la mise en ligne de la base de données sur un **serveur multi-utilisateurs** qui utilisera les protocoles sécurisés :
SCP (Secure CoPy)
SFTP (SSH File Transfer Protocol)
FTPS (FTP SSL/TLS)