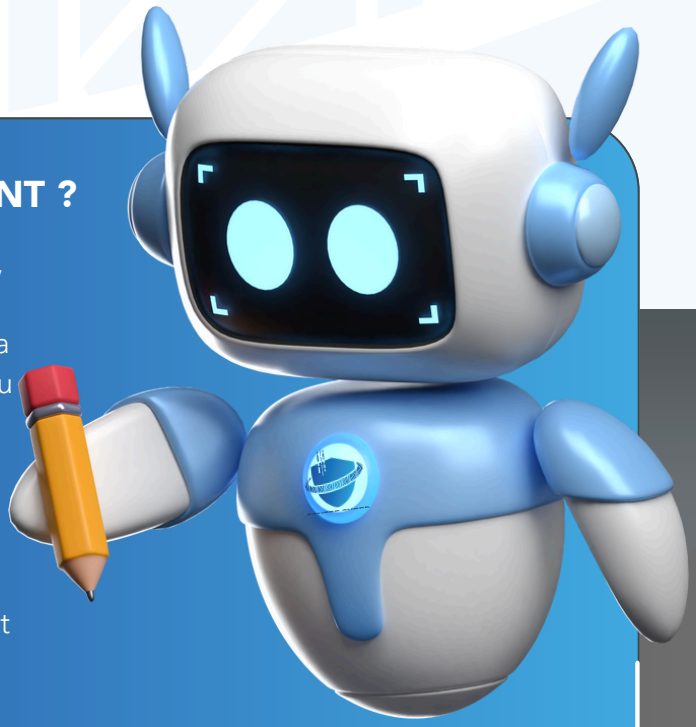
LES MOTS DE PASSE

CENTRE CYBER DU PACIFIQUE

EN BREF



POURQUOI C'EST IMPORTANT ?

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

1. UTILISEZ UN MDP DIFFÉRENT POUR CHAQUE SERVICE
2. UTILISEZ UN MDP SUFFISAMMENT LONG ET COMPLEXE
3. UTILISEZ UN MDP IMPOSSIBLE À DEVINER
4. UTILISEZ UN GESTIONNAIRE DE MDP
5. CHANGEZ VOTRE MDP AU MOINDRE SOUPÇON
6. NE COMMUNIQUEZ JAMAIS VOTRE MDP À UN TIERS
7. N'UTILISEZ PAS VOS MDP SUR UN ORDINATEUR PARTAGÉ
8. ACTIVEZ LA « DOUBLE AUTHENTIFICATION »
9. CHANGEZ LES MDP PAR DÉFAUT DES DIFFÉRENTS SERVICES
10. CHOISISSEZ UN MDP PLUS ROBUSTE POUR VOTRE MESSAGERIE

▶ Voir détail page "ADOPTEZ LES BONNES PRATIQUES"

LES MOTS DE PASSE

CENTRE CYBER DU PACIFIQUE

ADOPTEZ LES BONNES PRATIQUES

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

1. UTILISEZ UN MDP DIFFÉRENT POUR CHAQUE SERVICE

En cas de perte ou vol d'un mot de passe, seul le service concerné sera vulnérable. Sinon, tous les services utilisant ce même mot seraient compromis.

2. UTILISEZ UN MDP LONG ET COMPLEXE

Les attaques par « force brute » testent des milliers de combinaisons par seconde. Utilisez un MDP d'au moins 12 caractères, mélangeant majuscules, minuscules, chiffres et caractères spéciaux pour vous protéger.

3. UTILISEZ UN MDP IMPOSSIBLE À DEVINER

Les pirates tentent souvent de deviner votre MDP. Évitez les informations personnelles faciles à trouver (prénoms, dates, etc.) et les suites logiques (123456, azerty, abcdef).

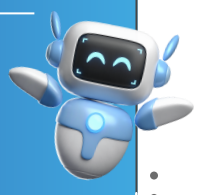
4. UTILISEZ UN GESTIONNAIRE DE MDP

Il est impossible de retenir de nombreux MDP complexes. N'écrivez pas vos MDP sur des pense-bêtes ou des fichiers non sécurisés. Utilisez un gestionnaire de MDP sécurisé qui les stocke pour vous. Voir encadré sur Keepass ci-dessous.

5. CHANGEZ VOTRE MDP AU MOINDRE SOUPÇON

Si vous doutez de la sécurité d'un compte ou que vous entendez parler d'un piratage d'un service que vous utilisez, changez immédiatement votre MDP pour éviter tout risque.

CRÉER UN MOT DE PASSE SOLIDE



LA MÉTHODE DES PREMIÈRES LETTRES
Un tien vaut mieux que deux tu l'auras
1tvmQ2tl'A

LA MÉTHODE PHONÉTIQUE
J'ai acheté huit CD pour cent euros cet après-midi
ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

KEEPASS UN GESTIONNAIRE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires. keepass.info

LES MOTS DE PASSE

CENTRE CYBER DU PACIFIQUE

ADOPTEZ LES BONNES PRATIQUES

6. NE COMMUNIQUEZ JAMAIS VOTRE MDP À UN TIERS

Votre MDP doit rester secret. Aucune société sérieuse ne vous le demandera par messagerie ou téléphone, même pour une maintenance. Si c'est le cas, considérez cela comme une tentative de piratage.

7. N'UTILISEZ PAS VOS MDP SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs publics peuvent être piégés pour récupérer vos MDP. Si vous devez utiliser un tel appareil, activez la navigation privée, fermez bien vos sessions et ne sauvegardez jamais vos MDP dans le navigateur. Changez vos MDP dès que vous revenez sur un ordinateur sûr.

8. ACTIVEZ LA DOUBLE AUTHENTIFICATION* LORSQUE C'EST POSSIBLE

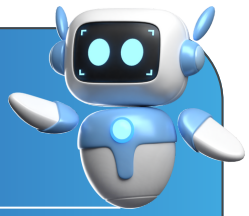
Pour renforcer vos accès, de nombreux services proposent cette option. En plus de votre MDP, une confirmation supplémentaire (code par SMS, e-mail, application, ou biométrie) vous est demandée, garantissant que vous seul pouvez accéder à vos comptes.

9. CHANGEZ LES MDP PAR DÉFAUT DES SERVICES

Certains services ont des MDP par défaut, souvent connus des cybercriminels. Changez-les rapidement pour des MDP que vous maîtrisez.

10. CHOISISSEZ UN MDP ROBUSTE POUR VOTRE MESSAGERIE

Votre messagerie est liée à de nombreux comptes en ligne, souvent utilisée pour la réinitialisation de MDP. Un pirate qui accède à votre messagerie pourrait compromettre vos autres comptes, d'où l'importance d'un MDP très sécurisé pour ce service.



QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook/Hotmail, Gmail, Yahoo Mail...
- Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter...
- Skype, Teams, WhatsApp, Zoom...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, OneDrive...

POUR ALLER PLUS LOIN

Par la CNIL : Les conseils de la CNIL pour un bon mot de passe
Par l'ANSSI : Sécurité des mots de passe

**Également appelée « authentification forte », « authentification multifacteurs », « 2FA », « vérification en deux étapes », « validation en deux étapes », « authentification à deux facteurs », « identification à deux facteurs », « vérification en deux temps »…*