

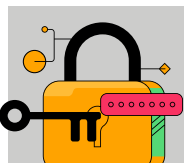
CYBER RÉFLEXES

CRÉER ET GÉRER VOS MOTS DE PASSE

1

CRÉEZ DES MOTS DE PASSE SUFFISAMMENT LONGS ET COMPLEXES

Un mot de passe, c'est une clé. Unique à chaque porte, elle vous protège de l'intrusion. Si vous utilisez la même clé ou une clé facile à reproduire, il sera facile pour un malfaiteur d'en tirer profit, pour ouvrir plusieurs portes.



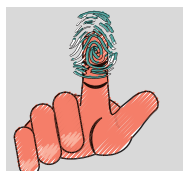
BONNES PRATIQUES

- Évitez d'y inclure des renseignements personnels.
- Utilisez au moins 12 caractères en incluant, de façon aléatoire, des majuscules, des chiffres et des caractères spéciaux.

3

CHOISISSEZ DES PHRASES/MOTS DE PASSE DIFFÉRENTS POUR CHAQUE COMPTE

Choisir le même mot de passe pour tous vos comptes facilite la vie aux cybercriminels... En créant des mots de passe à la fois robustes et uniques, vous pouvez mieux sécuriser vos comptes.



BONNES PRATIQUES

- Des outils comme les gestionnaires de mots de passe peuvent vous suggérer des mots de passe variés et forts.
- Vous préférez ne pas créer de mot de passe? Optez pour un mot de passe à usage unique, valable pour une session ou une transaction.

5

PROTÉGEZ VOS MOTS DE PASSE ET NE LES DIVULGUEZ PAS

La tentation de vouloir partager ses mots de passe peut parfois être grande... Mais à moins de ne devoir le faire via un système sécurisé pour le travail par exemple, il est primordial de ne jamais révéler vos mots de passe à qui que ce soit.



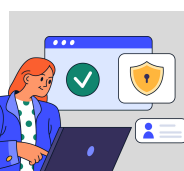
BONNES PRATIQUES

- Évitez de conserver une copie de vos mots de passe dans un lieu public, par exemple sous votre clavier ou collés sur le côté de votre ordinateur.
- Vous soupçonnez que votre mot de passe est connu d'une autre personne? Changez-le immédiatement.

2

LORSQUE POSSIBLE, UTILISEZ UNE PHRASE DE PASSE

Une phrase de passe est un amalgame de mots disparates qui n'ont de sens que pour vous. Unique, elle s'avère difficile voire impossible à deviner, mais est plus facile à retenir et à taper!



BONNES PRATIQUES

- Trouvez 4 mots uniques qui totalisent minimum 15 caractères.
- Vous pouvez y aller par association d'idées, par exemple 4 choses qui se trouvent devant vous ("lampeordinateurplantescadre").
- Vous pouvez aussi modifier des lettres de votre phrase par des symboles ou chiffres (C'3st l'h3ur3 du caf3!).
- Évitez les citations célèbres de littérature, chansons, films, etc.

4

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Avec lui, vous n'oublierez plus jamais vos mots de passe! Qu'il soit gratuit ou payant, il enregistre vos mots de passe de manière sécurisée et vous permet de vous connecter plus facilement.



BONNES PRATIQUES

- Exemples d'outils gratuits : 1Password, LastPass, Bitwarden ou encore celui de votre moteur de recherche.
- Assurez-vous d'avoir les fonctionnalités suivantes :
 - L'authentification multifactorielle
 - Une invitation à modifier les vieux mots de passe
 - La notification des mots de passe faibles ou déjà utilisés
 - L'intégration à vos autres appareils électroniques

Plus d'information sur
ulaval.ca/cybersecurite

Victime ou témoin d'une fraude?

Signalez-le rapidement au
Centre de cyberfédense ULaval



UNIVERSITÉ
LAVAL