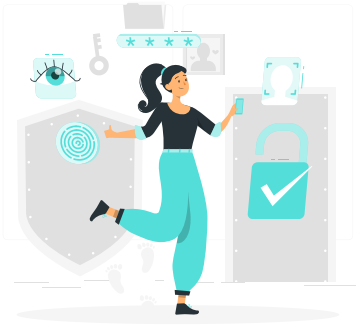
SÉCURISEZ VOS MOTS DE PASSE POUR PROTÉGER VOTRE ENTREPRISE

laboutic.fr
fiche pratique

Pourquoi sécuriser vos mots de passe ?

Les mots de passe sont la première ligne de défense contre les intrusions. Un mot de passe faible ou compromis expose vos données sensibles au risque de vol ou d'accès non autorisé. Assurer leur sécurité protège votre entreprise, vos clients et votre réputation. Ne négligez jamais cette barrière essentielle.



Définition

Un mot de passe est une séquence secrète de caractères permettant de confirmer l'identité d'un utilisateur lors de l'accès à un système ou service électronique. Il sert à protéger les informations et garantir que seules les personnes autorisées puissent accéder à certaines ressources.

En pratique

Complexité : Votre mot de passe devrait avoir au moins 12 caractères, comprenant des lettres majuscules, des lettres minuscules, des chiffres et des symboles.

Unicité : Chaque service ou site devrait avoir son propre mot de passe. Évitez de réutiliser le même mot de passe, afin que si l'un est compromis, les autres restent en sécurité.

Changements réguliers : Même si votre mot de passe est fort, il est conseillé de le changer tous les 3-6 mois. Cela réduit le risque qu'il soit compromis.

Évitez les évidences : Ne choisissez pas de mots de passe basés sur des informations facilement accessibles, comme votre nom, date de naissance ou le nom de l'entreprise.

Méthode mnémotechnique : Si vous craignez d'oublier un mot de passe complexe, pensez à une phrase que vous aimez ou un dicton, et utilisez la première lettre de chaque mot comme base de votre mot de passe.

En respectant ces conseils, vous assurez une meilleure protection de vos données à travers vos mots de passe.

La force des mots de passe

La force d'un mot de passe réside dans sa capacité à résister aux tentatives de devinettes ou de piratage. Elle dépend de sa longueur, de sa complexité et de son imprévisibilité.

D'ailleurs, une longueur minimale de 12 caractères est généralement recommandée, car elle offre une combinaison solide entre praticité et sécurité. Voici quelques exemples pour illustrer :

Faible : ananas
Pourquoi ? C'est un mot courant du dictionnaire sans variation de caractères.

Moyen : Ananas!98P
Pourquoi ? Bien qu'il contienne des lettres majuscules, des chiffres et un symbole, la base est toujours un mot courant.

Fort : a2N#4s!8zKp0
Pourquoi ? Il combine de manière imprévisible des lettres majuscules et minuscules, des chiffres et des symboles, et n'a pas de signification évidente.

Basé sur une phrase : J'aime le ciel bleu ! peut devenir JaLcB!9Pz
Pourquoi ? Utiliser les initiales d'une phrase est une technique mnémotechnique pour se rappeler des mots de passe compliqués.

L'idéal est de viser un niveau de force équivalent ou supérieur au troisième exemple. Les pirates utilisent des outils automatisés pour deviner les mots de passe en se basant sur des listes de mots courants, des noms, des dates, etc. Plus votre mot de passe est long et complexe, moins il est probable qu'il soit découvert.

Utilisez un gestionnaire de mots de passe

Un gestionnaire de mots de passe est comme un coffre-fort numérique pour tous vos codes secrets. Avec lui, plus besoin de retenir des dizaines de mots de passe : il les garde tous en sécurité. Vous n'avez qu'à vous souvenir d'un seul mot de passe, le "mot de passe maître", pour accéder à tous les autres. En plus, il peut créer pour vous des mots de passe forts et uniques pour chaque site. C'est donc un outil pratique qui renforce énormément votre sécurité en ligne.

Et après ?

Retrouvez tous nos conseils et la possibilité d'établir un pré-diagnostique gratuit de votre sécurité numérique sur notre site protectiondesentreprises.fr

protection des entreprises
ensemble, protégeons votre activité

**Besoin d'un conseil, d'un accompagnement...
contactez votre conseiller local**

CHAMBRE DE COMMERCE ET D'INDUSTRIE