

La meilleure défense contre l'ingénierie sociale ?

Un gestionnaire de mots de passe



Les entreprises prévoient que l'hameçonnage sera la plus grande menace d'ingénierie sociale en 2024¹.

81%

des entreprises constatent une augmentation de l'hameçonnage¹.

Il est essentiel pour la sécurité de votre organisation de garder une longueur d'avance sur les acteurs malveillants.

L'ingénierie sociale exploite les faiblesses humaines par manipulation psychologique.



L'éducation et la formation ont des limites. Le meilleur outil que vous pouvez fournir à vos employés pour déjouer l'ingénierie sociale ?

Un gestionnaire de mots de passe.

Avec un gestionnaire de mots de passe, vos employés :



Utilisent des mots de passe complexes

Un gestionnaire de mots de passe génère et stocke des **mots de passe robustes** pour chaque compte, diminuant le recours aux mots de passe trop simples et faciles à deviner. Qui dit plus dur à pirater dit plus dur à hameçonner.

Ne réutilisent jamais les mots de passe

Les **mots de passe uniques** protègent contre les accès illicites, même si l'ingénierie sociale parvient à obtenir une paire d'identifiants.



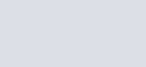
Éviter les sites frauduleux

Un gestionnaire de mots de passe limite la saisie des mots de passe aux sites vérifiés en **préremplissant** les identifiants. S'il ne les préremplit pas, c'est potentiellement un signe de tentative d'hameçonnage.



Armer vos employés d'un gestionnaire de mots de passe est essentiel pour assurer l'intégrité et la protection des données de votre entreprise face à la menace croissante de l'ingénierie sociale.

Vous pouvez diminuer la dépendance de votre organisation sur les comportements humains :



Gérez les mots de passe de manière centralisée



Partagez les mots de passe de manière simple et sûre



Passez au sans mot de passe lorsque vous êtes prêt



Avec plus d'un milliard de sites protégés, LastPass simplifie la sécurité en ligne pour des millions d'utilisateurs et 100 000 entreprises.

[Nous contacter](#)