



WP Atelier

Présentation du cours et de l'importance de la sécurité des mots de passe pour l'administration de WordPress.

Objectif : Expliquer comment composer un mot de passe fort et justifier son choix.

1. Importance d'un Mot de Passe Sécurisé

Risques liés à un mot de passe faible : piratage, accès non autorisé, perte de données.
Impact sur la sécurité globale du site et la protection des informations sensibles.



Bonnes Pratiques pour un Mot de Passe Fort (3:00 - 6:00)

Longueur : Un mot de passe doit comporter au moins 12 caractères.

Complexité : Utilisation de majuscules, minuscules, chiffres et caractères spéciaux.

Unicité : Ne pas réutiliser le même mot de passe pour plusieurs comptes.

Génération aléatoire : Utiliser des outils pour générer des mots de passe aléatoires.

[MÉDIATHÈQUE](#) | [GLOSSAIRE](#) | [BESOIN D'AIDE](#) | [PRESSE](#) | [FR](#) - [EN](#) | [GESTION DES COOKIES](#)

CNIL

[PARTICULIER](#) [JE SUIS UN PROFESSIONNEL](#)

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

[MA CONFORMITÉ AU RGPD](#) | [THÉMATIQUES](#) | [TECHNOLOGIES](#) | [TEXTES OFFICIELS](#) | [LA CNIL](#) [Q](#) [f](#) [t](#)

[Générer un mot de passe solide](#)

Générer un mot de passe solide

Cet outil vous aide à construire un mot de passe fort et simple à retenir.
Aucun mot de passe n'est récupéré par le site de la CNIL.

1

Choisir une phrase que vous retiendrez facilement

Exemples :

Mon mot de passe est un secret bien gardé depuis 25 ans !
Le rire seul échappe à notre surveillance. Natalie Clifford-Barney, 1920.
Le carré de l'hypoténuse est égal à la somme des carrés des 2 autres côtés.

En panne d'inspiration ?

Composition du Mot de Passe

Exemple de mot de passe : aB7!kL9@zX2#

Majuscules : A, B, L, X

Minuscules : a, k, z

Chiffres : 7, 9, 2

Caractères spéciaux : !, @, #

Explication de chaque composant et de son rôle dans la sécurité.

Majuscules (A, B, L, X) :

Rôle : Les majuscules augmentent la complexité du mot de passe en ajoutant une couche supplémentaire de caractères possibles. Cela rend le mot de passe plus difficile à deviner ou à cracker par des attaques par force brute.

Exemple : Dans aB7!kL9@zX2#, les majuscules sont dispersées, ce qui complique les tentatives de deviner le mot de passe.

Minuscules (a, k, z) :

Rôle : Les minuscules sont la base de la plupart des mots de passe, mais lorsqu'elles sont combinées avec d'autres types de caractères, elles contribuent à la diversité nécessaire pour un mot de passe fort.

Exemple : Les minuscules dans aB7!kL9@zX2# sont mélangées avec d'autres caractères, rendant le mot de passe moins prévisible.

Chiffres (7, 9, 2) :

Rôle : Les chiffres augmentent l'entropie du mot de passe, c'est-à-dire le nombre total de combinaisons possibles. Cela rend le mot de passe plus robuste face aux attaques automatisées.

Exemple : Les chiffres dans aB7!kL9@zX2# sont placés de manière aléatoire, ce qui accroît la difficulté de deviner le mot de passe.

Caractères Spéciaux (!, @, #) :

Rôle : Les caractères spéciaux sont cruciaux car ils ajoutent une complexité supplémentaire que beaucoup de mots de passe simples n'ont pas. Ils sont souvent négligés par les utilisateurs, ce qui les rend particulièrement efficaces pour renforcer la sécurité.

Exemple : Dans aB7!kL9@zX2#, les caractères spéciaux sont intégrés de manière à rendre le mot de passe unique et difficile à cracker.

Changement Régulier des Mots de Passe

Recommandation de changer les mots de passe régulièrement (tous les 3 à 6 mois).

Sensibilisation et Formation (15:00 - 17:00)

Importance de sensibiliser tous les utilisateurs ayant accès à l'administration du site.
sur les bonnes pratiques de sécurité.

Conclusion

Pour composer un mot de passe sécurisé.

Je vous encourage à adopter ces bonnes pratiques pour protéger l'accès à l'interface d'administration de votre WordPress.