

Sécuriser ses mots de passe

Un mot de passe faible, c'est une porte ouverte. Des milliers de comptes sont piratés chaque jour non pas par des hackers géniaux, mais parce que le mot de passe était trop simple ou réutilisé partout. Voici les trois réflexes qui changent tout.

01 Utiliser des mots de passe complexes et uniques

Les pirates utilisent des logiciels qui testent des millions de combinaisons par seconde. Un mot de passe court ou simple peut être cracké en quelques minutes.

Les règles de base :

Minimum **12 caractères**, avec majuscules, minuscules, chiffres et caractères spéciaux (! @ # \$ %...). Jamais votre prénom, date de naissance ou nom de votre animal — ce sont les premières choses testées par les pirates.

La technique de la phrase secrète :

"*Mon chat Félix a 3 ans !*" devient **McF@3ans!** — facile à retenir, très difficile à deviner. Ajoutez 3-4 caractères pour atteindre 12+.

Un mot de passe différent par site :

Si un seul site se fait pirater et que vous utilisez le même mot de passe partout, **tous vos comptes sont compromis d'un coup**. Un compte = un mot de passe unique.

À éviter : 'Azerty123', 'password', '123456', prénom + année. Ces mots de passe figurent dans les premières listes testées.

02 Activer la double authentification (2FA)

Même si quelqu'un vole votre mot de passe, il ne peut pas accéder à votre compte sans un **code à 6 chiffres** envoyé sur votre téléphone. Ce code change toutes les 30 secondes.

Sur Gmail :

Compte Google > **Sécurité** > **Validation en deux étapes** > Activer.

Sur Outlook/Microsoft :

account.microsoft.com > **Sécurité** > **Options avancées** > **Vérification en deux étapes**.

Sur Facebook / Instagram :

Facebook : **Paramètres** > **Sécurité et connexion** > **Authentification à deux facteurs**.

Instagram : **Profil** > **Paramètres** > **Sécurité** > **Authentification à deux facteurs**.

Bon à savoir : Commencez par votre messagerie. Si un pirate en prend le contrôle, il peut réinitialiser tous vos autres mots de passe — c'est le compte le plus critique.

03 Utiliser un gestionnaire de mots de passe

Retenir un mot de passe unique et complexe pour chaque site est impossible. Un gestionnaire les génère, les mémorise et les saisit à votre place. Vous n'avez plus qu'**un seul mot de passe à retenir** : celui du gestionnaire.

Bitwarden (gratuit, recommandé) :

Disponible sur PC, Mac, téléphone et en extension navigateur. Il génère des mots de passe forts et les remplit automatiquement sur les sites. Téléchargement sur **bitwarden.com**.

KeePass (gratuit, stockage local) :

Alternative idéale pour ceux qui ne veulent pas confier leurs mots de passe à un serveur distant. KeePass stocke tout dans un fichier chiffré sur votre propre ordinateur — rien n'est envoyé sur internet. Plus sécurisé en théorie, mais un peu moins intuitif que Bitwarden. Téléchargement sur **keepass.info** (version KeePassXC recommandée pour Windows et Mac).

Pour démarrer :

1. Créez un compte Bitwarden avec un mot de passe maître **très solide** (notez-le sur papier dans un endroit sûr — si vous le perdez, vous perdez tout). 2. Lors de chaque connexion, laissez Bitwarden enregistrer le mot de passe. 3. Progressivement, remplacez vos anciens mots de passe faibles par des mots de passe générés.

Bon à savoir : Votre navigateur (Chrome, Firefox, Edge) peut déjà enregistrer vos mots de passe. C'est moins sécurisé qu'un gestionnaire dédié, mais infiniment mieux qu'un post-it sous le clavier.

Vous avez un doute sur la sécurité de vos comptes ?

On fait un audit de vos accès et on vous aide à tout sécuriser, à distance ou à domicile.

Appelez-nous : 09.81.65.35.09