

LA MINUTE DU PSIR

GESTIONNAIRE DE MOTS DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise... la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. Au quotidien, gérer des dizaines d'identifiants est devenu une corvée.

Les gestionnaires de mots de passe visent précisément à nous l'épargner

Il s'agit d'outils permettant de **stocker à un seul endroit tous les mots de passe** que vous utilisez. Ils peuvent prendre la forme d'un **logiciel classique** ou d'une **simple extension dans le navigateur** (ils s'utilisent alors comme un site web).

Le principe de base de quasi tous les gestionnaires de mots de passe est simple : lorsque vous entrez votre identifiant et votre mot de passe sur un site, le gestionnaire le détecte et vous propose de le stocker. Cette sauvegarde **permet donc facilement d'avoir des mots de passe longs, complexes et même de les renouveler régulièrement** ! Lorsque vous vous rendez à nouveau sur le site, les champs de saisies seront préremplis.

Pour accéder à votre « coffre-fort », le gestionnaire vous demandera **un mot de passe maître**, généralement au démarrage. Il faut le **choisir avec soin** et recourir si possible à une « phrase de passe » : **ce sera la clé** qui déverrouillera l'accès aux autres mots de passe. Il faut prendre bien soin de ne pas l'oublier car sans elle, vous perdrez l'accès à tous vos autres mots de passe. Tous les gestionnaires **sécurisent les mots de passe en les chiffrant avant**, le cas échéant, de les sauvegarder en ligne – ce qui signifie que même en cas de piratage, les mots de passe dérobés seraient illisibles par les pirates.

Outre le stockage et le préremplissage des mots de passe, les gestionnaires disposent **d'une foule de fonctionnalités** qui varient selon le logiciel choisi : évaluation de la robustesse des mots de passe, générateur de mots de passe solides, stockage des identités (pour ne pas avoir à remplir systématiquement son adresse, son numéro de téléphone ou de carte bancaire sur les sites de vente en ligne), partage sécurisé de mots de passe...

Il existe des **solutions gratuites ou payantes** qui répondent à différents besoins.

Plusieurs critères sont à prendre en compte pour choisir son gestionnaire :

- **L'interface et l'ergonomie** : certains gestionnaires de mots de passe ont mis l'accent sur la facilité d'usage.
- **Sa sécurité** : un logiciel libre ou *open source* peut apporter des garanties supplémentaires en matière de sécurité car le code source aura été examiné et vérifié.
- **Sa disponibilité** sur les différents systèmes d'exploitation.

Les principaux gestionnaires sont Dashlane, RobotForm, NordPass, Enpass, Lastpass, 1password et Keepass qui a obtenu un **visa de sécurité par l'Agence Nationale de la Sécurité des Systèmes d'Information** (www.ssi.gouv.fr)

DIFFICULTÉ



THEMATIQUE

SECURITE INFORMATIQUE

PERSONNES CONSEILLÉES



LEARN MORE

Pour en savoir plus, cliquer ici

Pourquoi et comment bien gérer ses mots de passe ?

Comment fonctionne un gestionnaire de mots de passe

