

Gestionnaires de mots de passe

La plupart des cliniques auront à créer des comptes pour plusieurs applications différentes, utilisées au quotidien. Garder la trace des mots de passe et des noms d'utilisateur de ces applications peut alors en venir à constituer une tâche ardue. Les gestionnaires de mots de passe sont un excellent moyen de s'assurer que tous les mots de passe sont uniques, forts et sécurisés, tout en n'ayant à n'en mémoriser qu'un seul. Lors du choix d'un gestionnaire de mots de passe, il est important de penser aux mesures de sécurité, à la convivialité, aux fonctionnalités, à la restauration des données, à la réputation et à la tarification.

Mesures de sécurité

- Quel type de chiffrement cette application utilise-t-elle?
- L'application permet-elle l'authentification multifacteur (AMF)?

Convivialité

- Dans quelle mesure l'application est-elle facile à utiliser?
- Est-elle compatible avec de multiples plateformes? (Windows, macOS, Unix, iOS, Android, etc.)
- Fonctionne-t-elle dans les navigateurs? (Chrome, Edge, Firefox, Opera, etc.)

Caractéristiques et fonctionnalités

- L'application comprend-elle un générateur de mots de passe intégré?
- Peut-elle entrer automatiquement les renseignements qui vous sont demandés?
- Vérifie-t-elle si vos mots de passe ont été compromis?

Restauration

- À quelle fréquence l'application effectue-t-elle des sauvegardes pour garantir que vous ne perdiez aucun mot de passe?
- Existe-t-il un moyen pour des personnes de confiance d'accéder à votre compte en cas d'urgence?

Réputation

- L'entreprise à l'origine de l'application effectue-t-elle régulièrement des vérifications de sécurité externes?
- L'application a-t-elle de bons antécédents? (atteintes à la vie privée, vente de données, etc.)

Prix

- Forfaits gratuits/payants. S'il y a possibilité d'un essai gratuit, pouvez-vous tester l'application avant de payer?
- Combien de fonctionnalités obtenez-vous pour le prix?

Gestionnaires de mots de passe

Recommandations

Il existe, dans ce domaine, un certain nombre d'applications ayant déjà fait leurs preuves, dont les suivants :

- **1Password** : Très apprécié pour sa sécurité, sa facilité d'utilisation et son excellent soutien à la clientèle. Largement axé sur la protection de la vie privée, grâce à son architecture à divulgation nulle de connaissance.
- **Dashlane** : Offre des fonctionnalités complètes, y compris la surveillance du Web clandestin et des services VPN dans ses forfaits supérieurs. Convivial, il comporte de solides mesures de sécurité.
- **Bitwarden** : Logiciel ouvert hautement sécurisé offrant des options gratuites et supérieures. Il est reconnu pour sa transparence et pour la confiance que lui voue la communauté.
- **Keeper** : Très sécuritaire et doté de fonctionnalités telles que le stockage sécurisé des fichiers et la surveillance du Web clandestin. Offre une tarification concurrentielle et un soutien complet.