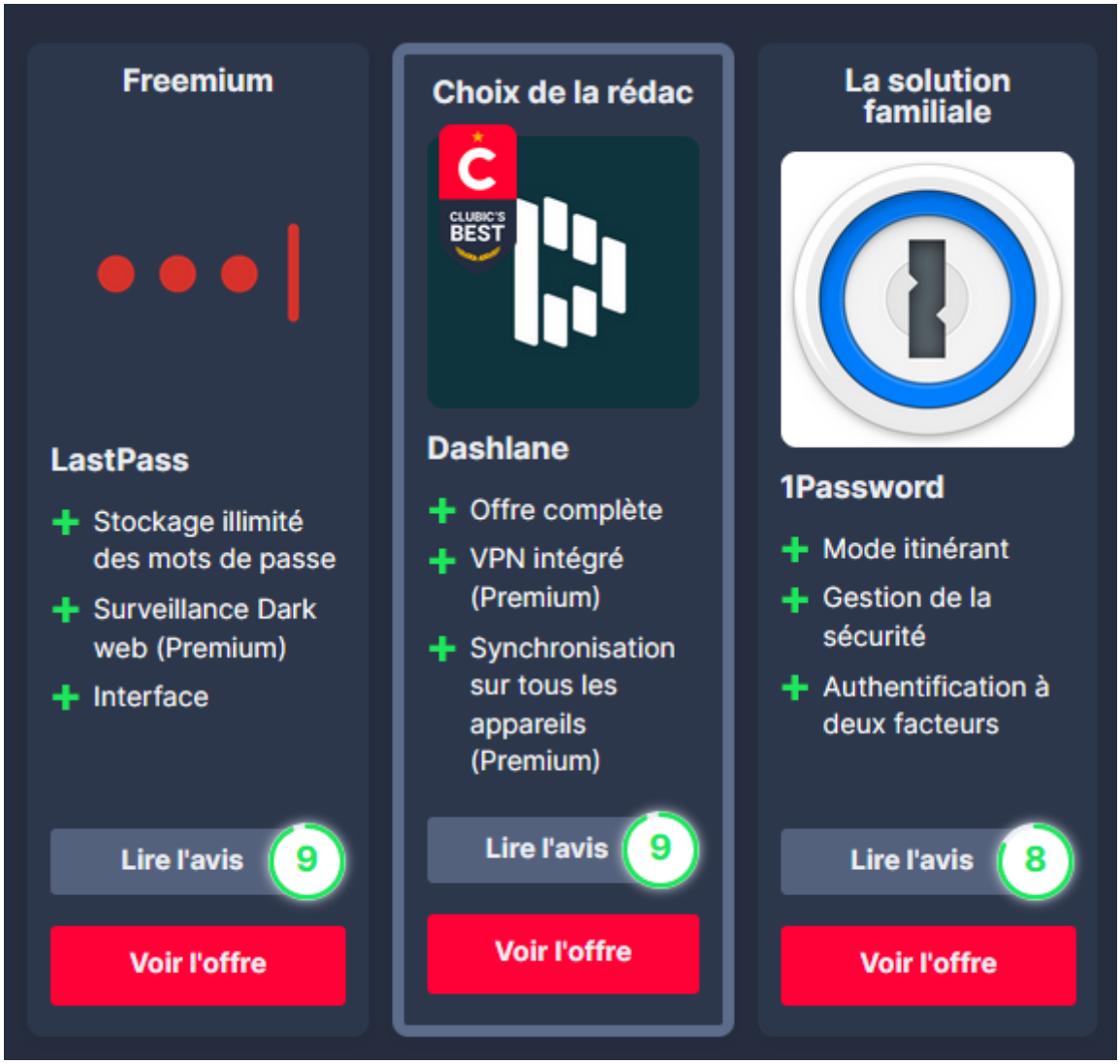
Comparatif des meilleurs gestionnaires de mots de passe (2022)

Malgré ses défauts, le mot de passe reste toujours le principal Sésame pour accéder à ses comptes et protéger ses données sensibles. Encore faut-il respecter quelques règles de base qui apparaissent comme autant de contraintes. Les deux principales sont la mémorisation et la gestion de mots de passe uniques. Avec un gestionnaire de mots de passe, ce n'est plus un casse-tête. L'offre étant maintenant très large, voici notre sélection.

Mots de passe écrits sur des post-it ou dans un tableau Excel, identiques pour plusieurs comptes, réduits à quelques caractères basiques comme un prénom et une date de naissance… Pour de nombreuses personnes, la gestion des mots de passe est un casse-tête. D'où ces pratiques très répandues, mais hélas très risquées. Pourtant, depuis des années, le Top 10 des mots de passe les plus utilisés dans le monde n'évolue pas beaucoup. Même chose en France.

Selon une étude menée par deux développeurs français, « 123456 », « 123456789 » et « azerty » composent le trio de tête des mots de passe les plus utilisés… Au risque de passer pour des rabat-joie, insistons encore sur le fait que ce type de mots de passe n'assure AUCUNE sécurité et confidentialité des données. Ils sont trop faciles à deviner et à trouver par des méthodes plus ou moins accessibles à tout le monde.



1. Lastpass : La solution ergonomique

Compatible Windows et MacOS mais aussi avec de nombreux navigateurs, LastPass est très facile à utiliser. Sa version gratuite permet de sauvegarder vos mots de passe, mais aussi vos informations sensibles.

Voir l'offre
Lire l'avis

LastPass

- Stockage illimité des mots de passe
- Surveillance Dark web (Premium)
- Interface

Avis de la rédaction

LastPass est très facile à maitriser. Tout est intuitif et bien organisé, que ce soit avec la version à installer sur ordinateur ou les applications mobiles. Comme d'autres gestionnaires en ligne, la version desktop offre plus de possibilités de réglages. Disponible gratuitement ou en version Premium (et Famille), LastPass répondra à tous vos besoins. Y compris, assurer la sécurité de vos logiciels installés sur un ordinateur sous Windows (version Premium). Sa documentation en français (mais pas les vidéos…) est complète et accessible. Dommage que sa version Premium n'intègre pas un VPN comme Dashlane.

Logiciel Freemium créé en 2008 et développé par l'éditeur américain LogMeIn, LastPass est une solution intuitive et claire. Vous pouvez l'utiliser de deux façons sur votre ordinateur. Soit en ajoutant cette extension pour chaque navigateur que vous disposez. Soit en installant la version de bureau pour Windows, macOS et même Linux.

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

2. Dashlane : Le plus ergonomique

Société américaine co-fondée par plusieurs Français en 2009, Dashlane propose une solution très complète et simple à utiliser. Son offre Premium garantit une synchronisation parfaite entre vos différents appareils. Cet éditeur n'a jamais connu de violation des données des utilisateurs. Une assurance tranquillité.

Voir l'offre
Lire l'avis

Dashlane

- Offre complète
- VPN intégré (Premium)
- Synchronisation sur tous les appareils (Premium)

Avis de la rédaction

Dashlane est un gestionnaire de mots de passe réputé pour ses performances et l'ergonomie de sa solution. Compatible avec les différents systèmes d'exploitation d'ordinateur et de smartphone, il propose une extension pour la majorité des navigateurs. La confidentialité de vos comptes est renforcée par différentes solutions d'authentification à multiples facteurs. Très complète, son offre Premium intègre aussi un VPN afin de limiter les risques de piratage lorsque vous vous connectez à vos sites depuis une borne Wi-Fi. Dommage que la version gratuite ne permette de stocker que 50 mots de passe.

Sur le papier, Dashlane propose les mêmes fonctionnalités que ses concurrents : création de mots de passe plus ou moins complexes, remplissage automatique de formulaires, partage de mots de passe… Dans la section Moyens de Paiements, vous pouvez enregistrer toutes les données de votre carte et les compléter automatiquement lors du paiement. Mais quelques points font la différence avec la concurrence.

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

3. 1Password : la solution pour une famille

Destiné dans un premier temps à l'écosystème d'Apple, il est dorénavant compatible avec la plupart des appareils, des navigateurs web et systèmes d'exploitation (MacOS, Windows, Linux), de sorte que vos mots de passe seront disponibles à tout moment, y compris sur les appareils mobiles (iOS, Android).

Voir l'offre
Lire l'avis

1Password

- Mode itinérant
- Gestion de la sécurité
- Authentification à deux facteurs

Avis de la rédaction

1Password propose des applications faciles à utiliser et perfectionnées qui fonctionnent sur ordinateur (Windows, MacOS et Chromebooks) et smartphones (iOS et Android). Sa fonction Watchtower vous aide à identifier et à modifier les mots de passe faibles, réutilisés ou compromis. Son « mode itinérant » reste original et pratique si vous allez dans des pays un peu trop curieux avec vos données personnelles. En cas de difficultés, vous pouvez contacter le support technique (par email, Twitter ou chat) qui est assez réactif et précis. Pour finir, 1Password est un bon gestionnaire pour une… famille ou un groupe d'utilisateurs professionnel. Pour un usage personnel et grand public, LastPass est plus adapté et gratuit.

À l'origine une application Premium pour MacOS uniquement, 1Password est maintenant compatible avec Windows et les systèmes d'exploitation iOS et Android. Sur le papier, cette solution partage de nombreuses fonctionnalités avec ses concurrents. Il y a cependant quelques différences.

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

4. Bitwarden : la sécurité au juste prix

Développée depuis 2016 par une petite équipe aux États-Unis, cette solution est open source et multiplateformes. Elle ne dispose pas d'autant de fonctionnalités que celles proposées par LastPass ou Dashlane, mais sa politique de sécurité est une référence. Et son offre Premium est vraiment accessible.

Voir l'offre
Lire l'avis

Bitwarden

- Politique de sécurité exemplaire
- Hébergement sur un NAS
- Offre Premium bon marché

Avis de la rédaction

Bitwarden est facile à utiliser, compatible avec Android et iOS et ses tarifs sont vraiment abordables. C'est aussi l'un des gestionnaires de mots de passe les plus sûrs, car son code source est accessible à tout le monde. Sa version gratuite offre les fonctionnalités de base dont vous avez besoin, y compris la possibilité de synchroniser autant de mots de passe que vous le souhaitez entre tous vos appareils, la prise en charge de l'authentification multiple (via une application ou une clé physique de type « Universal 2 Factor », YubiKey, Duo) et le partage. Dommage que sa version Premium n'intègre pas l'option « personne de confiance ».

Moins connu que d'autres poids lourds dans ce domaine, Bitwarden mérite qu'on s'y intéresse, car il ne manque pas d'atouts. Cette solution open source a mis en place une politique de sécurité exemplaire et son interface facilite son utilisation et les réglages. Bitwarden stocke vos identifiants de connexion, mais aussi vos identités, vos cartes bancaires et vos notes. Et plus encore….

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

5. NordPass : le jeune prometteur

NordPass assure très bien la mission pour laquelle il a été conçu : sécuriser l'accès à vos différents comptes en ligne en gérant vos mots de passe. Son interface est claire avec des menus explicites. Il lui manque peut-être le petit « plus » qui incitera les internautes à le choisir plutôt que les autres…

Voir le prix
NordPass

- Interface claire et efficace
- Niveaux de sécurité
- Authentification biométrique

NordPass est un très bon gestionnaire de mots de passe sans fioritures. Il assure le service qu'on lui demande : gérer ses mots de passe et quelques données sensibles. Ce service est simple, efficace et il bénéficie d'une politique de cybersécurité plus que correcte. Cependant, il manque peut-être d'ambition en ne proposant pas de fonctionnalités innovantes pour se démarquer de la concurrence. Par exemple, LastPass permet de gérer les codes d'accès et mot de passe de vos applications installées sur Windows tandis que la version Premium de Dashlane intègre un VPN.

L'éditeur de NordPass opère depuis le Panama, un pays qui ne fait pas partie des Five Eyes ni des Fourteen Eyes, des alliances d'agences de renseignement de plusieurs pays qui surveillent les activités des internautes pour protéger la sécurité nationale. Après un problème de sécurité rencontré en 2019 par NordVPN, l'éditeur a renforcé sa politique de chiffrement pour concevoir un gestionnaire de mot de passe digne de ce nom.

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

6. KeePass : la solution en « local »

Créé par l'allemand Dominik Reichl en 2003, KeePass est un gestionnaire de mots de passe uniquement en « local ». Vous devrez télécharger l'application et tous les modules complémentaires que vous souhaitez afin d'accéder à vos mots de passe.

Télécharger
Lire l'avis

KeePass

- Open source
- Version portable
- Nombreuses déclinaisons pour tous les OS

Avis de la rédaction

L'interface et l'utilisation de KeePass en feront peut-être fuir plus d'un. Mais ce logiciel gratuit répond parfaitement à ce qu'on lui demande en priorité : sauvegarder vos mots de passe. Autres atouts : une pléthore de plug-ins pour personnaliser son usage (interface, synchronisation cloud…). Il existe également des dizaines de déclinaisons pour tout appareil et système d'exploitation. Délivrée par l'Agence nationale de la sécurité des systèmes d'information pour des produits des technologies de l'information.

Apparu il y a 17 ans, KeePass fait figure de dinosaure avec son interface un peu vieillotte, son ergonomie pas vraiment intuitive au premier abord et l'absence de synchronisation entre différents appareils (c'est en effet un logiciel qui stocke en local vos mots de passe). Une fois qu'on a écrit ces quelques lignes, on peut se demander si KeePass doit être encore utilisé en 2021. La réponse est oui ! Présentons ses principaux atouts.

Offre, interface ergonomie, sécurité et fonctionnalités additionnelles

De quelques secondes à plusieurs années

Avec un ordinateur grand public, un mot de passe comme PassWord1 peut être trouvé en une poignée de secondes. Par contre, dès que l'on passe à des mots de passe supérieurs à 10 caractères (comprenant des symboles, des minuscules et des majuscules ainsi que des chiffres), le temps pour le casser passe à plusieurs mois, voire des années !

On comprend mieux l'intérêt de disposer de mots de passe en béton pour protéger vos données personnelles (numéro de carte bancaire, numéro de Sécurité Sociale, RIB...) et les accès à vos différents comptes en ligne. Entre les mains d'escrocs, tous ces éléments permettent d'usurper des identités, de faire du racket ou d'effectuer des achats sur le web...

Pour protéger vos informations, il est donc nécessaire de choisir et d'utiliser des mots de passe « forts », c'est-à-dire difficile à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Comment choisir ses mots de passe ?

- Utiliser un mot de passe unique pour chaque service.
- Choisir un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
- Ne pas demander à un tiers de générer pour vous un mot de passe.
- Modifier systématiquement, et le plus tôt possible, les mots de passe par défaut lorsque les systèmes en contiennent.
- Renouveler vos mots de passe avec une fréquence raisonnable (tous les 9 à 12 mois par exemple).
- Ne pas s'envoyer ses mots de passe sur sa messagerie personnelle.
- Configurer les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe.

Si vous êtes convaincus de l'intérêt d'avoir des mots de passe plus costauds, il reste à franchir une étape supplémentaire pour mettre ces conseils en pratique : utiliser un gestionnaire de mots de passe. Installés sur votre ordinateur (et votre smartphone) ou accessibles en ligne via une extension, ces logiciels vous éviteront d'avoir une grosse migraine : ils créent à votre place des mots de passe complexes et uniques. Plus la peine, de se prendre la tête à vouloir les apprendre par cœur ; il vous suffit de n'en retenir qu'un seul appelé « Mot de passe maitre » (ou « passphrase »). C'est en quelque sorte la grosse clé d'une commode qui permet d'ouvrir tous les petits tiroirs contenant chacun un mot de passe. Mais comment créer un mot de passe maitre et s'en souvenir ? Il existe différentes techniques de mémorisation. La première est appelée la méthode « phonétique ». Elle consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am.

La plus simple à notre avis est la méthode des « premières lettres » en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2Tl'a. Pour tester votre phrase, rendez-vous sur cette page de la CNIL.

Cryptage AES 256 bits

Dernière étape pour renforcer la confidentialité de vos comptes, utiliser un gestionnaire de mot de passe. Il existe des dizaines de « coffres-forts » répartis en deux catégories. La première est celle des gestionnaires en ligne qui synchronisent vos données sensibles (mots de passe, mais aussi n° de carte bancaire, adresse postale…) entre tous vos appareils. La seconde catégorie est celle des gestionnaires hors ligne qui stockent votre base de données de mots de passe sur votre ordinateur (ou, dans certains cas, sur une clé USB pour leur version portable).

Bien qu'il y ait un risque accru inhérent à chaque fois que vous stockez votre mot de passe en ligne, les gestionnaires de mots de passe basés sur le cloud stockent généralement les données sous la forme d'un fichier crypté sécurisé qui ne peut être ouvert que sur votre ordinateur. Différents critères permettent de retenir celui qui vous conviendra le mieux en fonction de vos besoins. Le premier concerne le niveau de cryptage utilisé pour protéger vos données contre les accès non autorisés. La majorité de ce type de service en ligne utilise un cryptage AES 256 bits. Certains gestionnaires de mots de passe utilisent également d'autres techniques comme le hashtag qui consiste à brouiller un mot de passe.

La compatibilité des appareils (PC et smartphones) et des navigateurs ainsi que le stockage illimité de données sont également des critères importants. Autre fonctionnalité pratique : la saisie automatique du login/password lorsque vous vous connectez à un compte en ligne. La capture automatique des mots de passe est également très pratique. Convaincu par nos conseils, vous allez devoir certainement changer la plupart de vos mots de passe et les intégrer dans votre gestionnaire. Une tâche plus ou moins fastidieuse, mais que vous ne ferez qu'une seule fois dans un premier temps (puis tous les neuf mois – ou une fois par an - pour effectuer un renouvellement qui est conseillé).

Pas de risque 0

Deux solutions dans ce cas : soit vous ouvrez votre gestionnaire et créez un password aléatoire que vous vous copiez ensuite dans la rubrique « Modifier mon mot de passe » du compte en question. En rentrant un nouveau mot de passe, le gestionnaire le repère et vous propose de l'enregistrer automatiquement dans sa base.

Certains gestionnaires de mots de passe ont inclus une notification automatique (par courrier électronique, dans l'application ou les deux) lorsqu'une violation se produit sur un service que vous utilisez. Ces notifications sont très utiles pour se tenir au courant des changements de mots de passe nécessaires.

Enfin, les fonctions d'importation et d'exportation ne sont pas à négliger, surtout si vous décidez de changer de gestionnaire de mots de passe ou de sauvegarder sur un disque dur (avec une partition ou un dossier chiffré) votre base de données.

Quelle que soit la solution retenue, elle ne garantit pas une sécurité à 100% si vous ne choisissez pas des mots de passe « forts » (d'ailleurs, certains gestionnaires vous avertissent quand ils sont trop faciles à trouver) et si vous n'êtes pas un peu vigilant lorsque vous recevez des emails usurpant une marque ou un site (phishing).

Cloud en panne

Enfin, ne mettez pas vos œufs dans le même panier. Même si la plupart des gestionnaires de mots de passe en ligne ont mis en place une politique de sécurité efficace, personne n'est à l'abri d'un bug ou d'une attaque Ddos paralysant son activité. Aucune entreprise, même des poids lourds comme Microsoft ou Google (avec des pannes plus ou moins longues de leurs services en ligne), n'est pas à l'abri. C'est la raison pour laquelle, nous vous recommandons de stocker en local (avec KeePass) vos mots de passe : vous pourrez toujours accéder à vos comptes personnels même si Dashlane ou LastPass par exemple sont inaccessibles pendant quelque temps.

Voici notre sélection. Toutes les solutions présentées partagent de nombreux points forts et fonctionnalités. Il est donc difficile d'établir un classement, car elles se tiennent dans un mouchoir de poche. Les quelques points différenciants sont minimes : une affinité ou non avec l'interface, les tarifs et le contenu des versions Premium.

Voir l'article entier sur le site CLUBIC.com :

https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel-gratuit-windows.html