Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

7 nov, 2026 · @Gabriel

Objectif : *Remplacer le gestionnaire de mots de passe de votre navigateur (Chrome, Edge, Safari), LastPass ou Dashlane par une solution libre et open source, chiffrée de bout en bout, dont vous choisissez l'hébergement.*

- ***Public visé :*** *Débutant à Intermédiaire*
- ***Temps estimé :*** *15 à 30 minutes (selon la solution choisie)*
- ***Difficulté :*** ★★☆☆☆ *(Facile à Moyen)*
- ***Prérequis :*** *aucun*
- ***Fiches associées :*** *N°7 (stockage), N°13 (Linux), N°18 (double authentification)*

1. Pourquoi quitter le gestionnaire de mots de passe de votre navigateur ? (Le problème)

Problème	Explication
Synchronisation via un compte big tech	Chrome ↔ compte Google, Edge ↔ compte Microsoft, Safari ↔ iCloud. Vos mots de passe dépendent de ces comptes.
Enfermement	Vos identifiants restent liés à un navigateur et à un écosystème.
Fonctions limitées	Peu ou pas de partage sécurisé, de notes chiffrées, de remplissage dans les applications hors navigateur selon les cas.
Logiciels privateurs	Pour Edge et Safari, le code n'est pas publié : impossible de vérifier ce qu'il fait de vos secrets.
Compte unique = point de défaillance	Si votre compte Google, Microsoft ou Apple est piraté, tous vos mots de passe sont exposés.

Le risque : vos identifiants dépendent d'un compte big tech ; s'il est compromis ou suspendu, vous perdez la main.

Le bénéfice : un gestionnaire **open source**, **chiffré de bout en bout**, dont vous **choisissez l'hébergement** (fichier local, auto-hébergement, ou serveurs en Europe ou en Suisse).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

2. Les trois grandes solutions libres et recommandées

Solution	Modèle	Open source	Chiffrement	Synchronisation	Idéal pour
Bitwarden	Cloud (serveurs aux États-Unis **ou dans l'UE**) ou auto-hébergement	✅ Oui	AES-256	✅ Native	Usage courant, plusieurs appareils, familles, débutants
KeePass / KeePassXC	Local (fichier .kdbx)	✅ Oui	AES-256 / ChaCha20	❌ Manuelle (fichier à synchroniser)	Contrôle total, aucun compte en ligne
Proton Pass	Cloud (Proton, Suisse)	✅ Oui	De bout en bout	✅ Native	Utilisateurs Proton (Mail, Drive, VPN)

Les trois solutions ont une version gratuite, avec des options payantes (partage familial, fonctions avancées).

3. Comparatif détaillé

Critère	Bitwarden	KeePass / KeePassXC	Proton Pass
Version gratuite	✅ Mots de passe illimités, **appareils illimités**	✅ Sans limite	✅ Mots de passe illimités, **appareils illimités**, 2 coffres, 10 alias e-mail
Applications mobiles officielles	✅ iOS / Android	⚠️ Applications tierces (KeePassDX, Keepass2Android, KeePassium, Strongbox)	✅ iOS / Android
Extension navigateur	✅	⚠️ KeePassXC-Browser (avec KeePassXC)	✅
Auto-hébergeable	✅ (serveur officiel ou Vaultwarden)	✅ (simple fichier)	❌
Compte en ligne requis	✅ (e-mail)	❌	✅ (compte Proton)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

Critère	Bitwarden	KeePass / KeePassXC	Proton Pass
Serveurs	États-Unis ou Union européenne (au choix à la création du compte)	Aucun	Suisse
Codes 2FA intégrés (TOTP)	Payant	✅ (KeePassXC)	Payant
Surveillance des fuites	Payant	⚠️ Via outils tiers	Payant
Partage	✅ Gratuit avec **1 autre personne** (organisation gratuite)	❌ (fichier partagé, peu pratique)	Payant
Générateur de mots de passe	✅	✅	✅

4. Comment choisir ? (Selon votre profil)

Si vous êtes...	Choisissez...	Pourquoi
Débutant, plusieurs appareils	**Bitwarden** (serveur UE)	Simple, gratuit sur tous vos appareils, extension intuitive.
Exigeant, vous voulez le contrôle total	**KeePassXC**	Fichier local, aucun serveur, aucun compte.
Déjà utilisateur Proton	**Proton Pass**	Écosystème intégré, Suisse.
Vous voulez auto-héberger	**Bitwarden** (Vaultwarden)	Léger, déployable avec Docker.
Vous ne voulez aucun compte en ligne	**KeePassXC**	Zéro compte, zéro cloud.

5. Méthode A : Bitwarden (recommandé pour la majorité des débutants)

Pourquoi Bitwarden ?

- **Simple** : extension navigateur + application mobile, synchronisation automatique.
- **Gratuit** : mots de passe et appareils illimités.
- **Open source** : code publié et audité.
- **Serveurs au choix** : États-Unis ou **Union européenne**.
- **Auto-hébergeable** : serveur officiel ou Vaultwarden (compatible, non officiel).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

Comment faire ? (Pas à pas)

Étape 1 : Créez un compte Bitwarden (sur le serveur européen)

1. Rendez-vous sur **bitwarden.com** → créer un compte.
    - Vous devez voir : le formulaire d'inscription avec un menu de **serveur / région**.
2. Choisissez la région **UE** (bitwarden.eu) dans ce menu.
    - Vous devez voir : la région européenne sélectionnée. ⚠️ Ce choix est définitif pour le compte.
3. Saisissez e-mail, nom et **mot de passe maître**.
    - Vous devez voir : la confirmation de création du compte.
4. **Notez votre mot de passe maître sur papier** et rangez-le en lieu sûr : c'est le seul que vous devez retenir, et Bitwarden ne peut pas le récupérer pour vous.
5. Vérifiez votre adresse e-mail.

Étape 2 : Installez Bitwarden sur vos appareils

Appareil	Action
Navigateur	Extension Bitwarden (Firefox, Brave…). Connectez-vous en choisissant la même région (UE).
Ordinateur (application)	Application de bureau sur **bitwarden.com/download** (Windows, macOS, Linux).
Android	F-Droid ou Aurora Store → « Bitwarden ».
iPhone	App Store → « Bitwarden ».

Installation sur Linux Mint (application de bureau)

Méthode 1 – Via la Logithèque (Flatpak, recommandée)

- Ouvrez la **Logithèque**, cherchez « Bitwarden », installez la version Flatpak (Flathub).
- ⚠️ Linux Mint bloque volontairement **snap** : la commande **sudo apt install snapd** échoue (« aucun candidat »). N'utilisez pas la méthode snap.

Méthode 2 – Via AppImage (portable)

1. Sur **bitwarden.com/download**, téléchargez le fichier .AppImage pour Linux.
2. Ouvrez un terminal dans le dossier de téléchargement.
3. Rendez-le exécutable : **chmod +x Bitwarden-*.AppImage**
4. Lancez-le : **./Bitwarden-*.AppImage**

Méthode 3 – Extension navigateur (la plus simple)

- Firefox : **Menu › Extensions et thèmes** → recherchez « Bitwarden » → **Ajouter à Firefox**.
- Connectez-vous avec votre compte (région UE).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

💡 **Recommandation :** pour débuter, l'extension navigateur suffit.

Étape 3 : Importez vos mots de passe existants

1. Exportez vos mots de passe depuis votre navigateur au format CSV (gestionnaire de mots de passe du navigateur → Exporter).
2. Dans Bitwarden : **Outils › Importer des données** → choisissez le format (ex. « Chrome (csv) », « Firefox (csv) »).
3. Importez le fichier.
4. **Supprimez le fichier CSV** (il n'est pas chiffré) et videz la corbeille.

Étape 4 : Changez vos mots de passe faibles

- Supprimez les doublons.
- Remplacez les mots de passe courts ou réutilisés.
- Générez un mot de passe unique par site avec le **générateur** intégré (ex. **xK9#mP2$vL7*QwR**).

Étape 5 (optionnel) : Auto-hébergement avec Vaultwarden (avancé)

Prérequis : Docker sur un serveur (Raspberry Pi, VPS, vieux PC) **et un accès en HTTPS** (Bitwarden refuse les connexions non sécurisées).

- Image Docker : **vaultwarden/server:latest**
- Variables utiles : **DOMAIN=https://votre-domaine.fr** et **SIGNUPS_ALLOWED=false** (après avoir créé votre compte).
- Données : montez un dossier persistant sur **/data/**.

Vaultwarden est une réimplémentation communautaire compatible, non officielle. Réservé aux utilisateurs avancés.

Limites de la version gratuite

- Pas de codes 2FA intégrés (TOTP), pas de rapports sur la santé du coffre, pas de pièces jointes chiffrées : ce sont des fonctions Premium.
- Partage limité à **une autre personne** (organisation gratuite).
- Premium : **19,80 $/an** depuis 2026 (renouvellements au nouveau tarif).

Pour la plupart des particuliers, la version gratuite suffit largement.

6. Méthode B : KeePassXC (contrôle total, aucun cloud)

Pourquoi KeePass / KeePassXC ?

- **Zéro cloud** : votre base est un fichier local (.kdbx).
- **Zéro compte** : pas d'e-mail, pas de serveur.
- **Fichier chiffré** (AES-256 ou ChaCha20).
- **Open source** et mature (KeePass existe depuis plus de 20 ans).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

- **KeePassXC** : version moderne et multiplateforme (Windows, macOS, Linux), compatible avec le format KeePass, avec codes 2FA intégrés et extension navigateur.

Comment faire ? (Pas à pas)

Étape 1 : Installez KeePassXC sur votre ordinateur

Système	Action
Windows	Téléchargez KeePassXC sur **keepassxc.org** (ou KeePass « classique » sur keepass.info).
macOS	Téléchargez KeePassXC sur **keepassxc.org**.
Linux Mint	Logithèque → « KeePassXC », ou **sudo apt install keepassxc**.

Étape 2 : Créez votre base de mots de passe

1. Lancez KeePassXC → **Créer une nouvelle base de données**.
2. Choisissez un **mot de passe maître très fort** (phrase de passe de 5 à 6 mots aléatoires).
    - Notez-le sur papier, rangé en lieu sûr. Sans lui, la base est perdue définitivement.
3. Choisissez l'emplacement du fichier .kdbx (ex. Documents/motsdepasse.kdbx).
4. (Optionnel) Ajoutez un **fichier-clé** : plus sûr, mais plus délicat à restaurer.

Étape 3 : Installez un client sur vos autres appareils

Appareil	Client recommandé
Android	KeePassDX (F-Droid) ou Keepass2Android
iPhone	KeePassium ou Strongbox (versions gratuites limitées)
Navigateur	KeePassXC-Browser (nécessite KeePassXC sur l'ordinateur)

Étape 4 : Synchronisez votre fichier .kdbx (optionnel)

Méthode	Niveau
Nextcloud (fiche N°7)	Facile : déposez le fichier dans votre dossier Nextcloud.
Syncthing (pair-à-pair)	Intermédiaire : synchronisation directe sans serveur.
Clé USB	Très simple : copie manuelle de temps en temps.

⚠️ Le fichier .kdbx est chiffré avant de quitter votre ordinateur : même stocké sur un cloud, il reste illisible sans votre mot de passe maître. Évitez seulement de le modifier sur deux appareils à la fois.

Étape 5 : Importez vos mots de passe

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

1. Exportez vos mots de passe depuis votre navigateur (CSV).
2. Dans KeePassXC : **Base de données › Importer › CSV**.
3. **Supprimez le fichier CSV** non chiffré.

Limites de KeePass

- Pas de synchronisation automatique (à organiser vous-même).
- Remplissage automatique moins intégré que Bitwarden (via KeePassXC-Browser).
- KeePass « classique » (Windows) a une interface plus ancienne ; KeePassXC est plus agréable.

7. Méthode C : Proton Pass (pour les utilisateurs de Proton)

Pourquoi Proton Pass ?

- **Intégré à l'écosystème Proton** (Mail, Drive, VPN).
- **Chiffré de bout en bout**, **open source**.
- **Serveurs en Suisse**.
- **Version gratuite généreuse** : mots de passe et appareils illimités, 2 coffres, **10 alias e-mail**.

Comment faire ? (Pas à pas)

1. Créez un compte gratuit sur **proton.me** (ou utilisez votre compte existant) et notez votre phrase de récupération.
    - Vous devez voir : votre tableau de bord Proton.
2. Installez Proton Pass :

Appareil	Action
Navigateur	Extension « Proton Pass » (Firefox, Brave…).
Ordinateur	Application de bureau sur **proton.me/pass/download**.
Android	Aurora Store → « Proton Pass » (ou fichier APK officiel de Proton).
iPhone	App Store → « Proton Pass ».

1. Importez vos mots de passe : dans les réglages de Proton Pass → **Importer** → choisissez votre navigateur ou un fichier CSV.
    - Vous devez voir : vos identifiants dans le coffre.
2. (Optionnel) Créez des **alias e-mail** pour vos inscriptions, afin de ne pas donner votre adresse réelle.

Limites de la version gratuite

- 10 alias e-mail, 2 coffres.

gabriel.ananda@mailo.com
CC BY SA

- Codes 2FA intégrés, surveillance des fuites (dark web) et partage avancé : offre payante **Pass Plus** (2,99 $/mois, facturé à l'année).

8. Tableau récapitulatif (gratuit / payant)

Fonctionnalité	Bitwarden gratuit	Bitwarden Premium (19,80 $/an)	KeePassXC	Proton Pass gratuit	Proton Pass Plus
Mots de passe illimités	✅	✅	✅	✅	✅
Appareils	Illimités	Illimités	Illimités	Illimités	Illimités
Codes 2FA intégrés	❌	✅	✅	❌	✅
Surveillance des fuites	❌	✅	❌ (outils tiers)	❌	✅
Partage	1 personne	✅	❌	⚠️ Limité	✅
Auto-hébergement	✅	✅	✅	❌	❌
Alias e-mail	❌	⚠️ Via un service tiers	❌	✅ (10)	✅

9. Cas particulier : KeePass et la synchronisation

Méthode	Difficulté	Compatibilité
Fichier .kdbx dans un dossier Nextcloud (fiche N°7)	Facile	Ordinateur + mobile (application Nextcloud)
Syncthing	Intermédiaire	Tous appareils, sans serveur
Clé USB	Très simple	Pas de synchronisation automatique
FreeFileSync	Facile	Copie programmée vers un disque externe

💡 **Pour débuter avec KeePass :** déposez votre .kdbx dans un dossier Nextcloud (hébergeur de confiance, ou Frama.space si vous êtes une association). Sur mobile, ouvrez-le avec KeePassDX via l'application Nextcloud.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

10. À savoir avant de se lancer

Crainte fréquente	La réalité
« Je vais tout perdre si j'oublie mon mot de passe maître. »	C'est vrai pour **tous** les gestionnaires. Notez-le sur papier, rangé en lieu sûr.
« Bitwarden est américain. »	Il est open source et propose des **serveurs dans l'UE**. Ou choisissez KeePassXC (aucun cloud) ou Proton Pass (Suisse).
« KeePass a l'air compliqué. »	Essayez **KeePassXC**, plus moderne, ou commencez par Bitwarden.
« Puis-je utiliser plusieurs gestionnaires ? »	C'est déconseillé (doublons, désynchronisation). Choisissez-en un.
« Et le partage avec ma famille ? »	Bitwarden gratuit permet de partager avec une personne ; au-delà, offres Familles payantes (Bitwarden, Proton).

11. Challenge 7 jours

Challenge : pendant 7 jours, utilisez votre nouveau gestionnaire **exclusivement**.

- **Jour 1 :** installez Bitwarden, KeePassXC ou Proton Pass.
- **Jour 2 :** importez vos mots de passe et supprimez le fichier CSV.
- **Jour 3 :** installez l'application mobile.
- **Jour 4 :** changez les 5 mots de passe les plus faibles.
- **Jour 5 :** utilisez le générateur à chaque nouvelle inscription.
- **Jour 6 :** supprimez les mots de passe enregistrés dans votre navigateur et désactivez sa proposition d'enregistrement.
- **Jour 7 :** activez la double authentification sur votre gestionnaire (fiche N°18).

Vous allez constater :

- Vous ne tapez plus de mots de passe (sauf le maître).
- Chaque site a un mot de passe unique et robuste.

12. Alternatives et approfondissements

Si vous avez besoin de…	Essayez plutôt…
Une solution 100 % hors ligne et portable	**KeePassXC** sur clé USB (éventuellement chiffrée avec VeraCrypt)
Une solution pour toute la famille	**Bitwarden Familles** ou **Proton Pass** (offres payantes)
Auto-héberger votre gestionnaire	**Vaultwarden** ou **KeePassXC** (fichier)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

Si vous avez besoin de…	Essayez plutôt…
Une solution pour une entreprise	**Bitwarden** (offres professionnelles)
L'extension navigateur la plus simple	**Bitwarden** ou **Proton Pass** (KeePassXC demande KeePassXC-Browser)

13. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Utiliser **Bitwarden** (serveur UE)	Gestionnaire simple, gratuit sur tous vos appareils	§ 5
Utiliser **KeePassXC**	Contrôle total, zéro cloud, zéro compte	§ 6
Utiliser **Proton Pass**	Intégré à Proton (Suisse), alias e-mail	§ 7
Quitter le gestionnaire du navigateur	Vos mots de passe ne dépendent plus d'un compte big tech	§ 1
Un mot de passe unique par site	Un site piraté ne compromet pas les autres	§ 5

À retenir absolument

- **Votre mot de passe maître est la clé de tout** : perdez-le, et vous perdez l'accès.
- Notez-le sur **papier**, rangé en lieu sûr ; ne le stockez pas en ligne en clair.
- **Un mot de passe unique par site** : c'est la règle d'or.
- N'importe laquelle de ces trois solutions vaut mieux que le gestionnaire du navigateur ou la réutilisation d'un même mot de passe.

Test final :

1. Créez un compte sur un site avec un mot de passe généré par votre gestionnaire.
2. Déconnectez-vous.
3. Reconnectez-vous grâce au remplissage automatique.
4. Vérifiez que le mot de passe apparaît aussi sur votre téléphone.
5. Si tout fonctionne : **vous avez réussi** ✅

Références

- Bitwarden – Offres du gestionnaire de mots de passe
- Bitwarden – Régions de serveurs (États-Unis, UE)
- AlternativeTo – Bitwarden Premium passe à 19,80 $/an (2026)
- Proton Pass – Tarifs et offre gratuite
- OMG! Ubuntu – Snap bloqué par défaut dans Linux Mint

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.2

- KeePassXC – site officiel
- Vaultwarden – dépôt officiel

gabriel.ananda@mailo.com
CC BY SA