

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

**Objectif :** Remplacer le gestionnaire de mots de passe de votre navigateur (Chrome, Edge, Safari), LastPass ou Dashlane par une solution libre, open-source et respectueuse de votre vie privée, qui ne stocke pas vos secrets sur des serveurs américains non contrôlés.

**Public visé :** Débutant à Intermédiaire

**Temps estimé :** 15 à 30 minutes (selon la solution choisie)

**Niveau de difficulté :** ★★☆☆☆ (Facile à Moyen)

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

Problème	Explication
<b>Mots de passe stockés en clair</b> (parfois)	Certains navigateurs (notamment les anciennes versions) stockent les mots de passe sans chiffrement ou avec un chiffrement faible.
<b>Synchronisation via un compte big tech</b>	Chrome ↔ compte Google, Edge ↔ compte Microsoft, Safari ↔ iCloud. Vos mots de passe transitent par leurs serveurs.
<b>Pas de logiciel dédié</b>	Un navigateur n'est pas un coffre-fort. Pas de générateur de mot de passe robuste, pas de vérification de fuite de données, pas de remplissage hors navigateur (applications).
<b>Failles de sécurité historiques</b>	Chrome, Edge et Safari ont eu des vulnérabilités exposant les mots de passe en clair.
<b>Logiciels privés</b>	Vous ne savez pas ce que le code fait réellement avec vos secrets.

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

**Le risque :** Vos identifiants sont stockés sur des serveurs américains, potentiellement analysés, et vulnérables en cas de piratage de votre compte Google/Microsoft/Apple.

**Le bénéfice :** Un gestionnaire de mots de passe **open-source, chiffré de bout en bout**, et dont vous pouvez **choisir l'hébergement** (cloud local, auto-hébergement, ou serveurs de confiance européens).

### 2. Les trois grandes solutions libres et recommandées

Solution	Modèle	Open-source	Chiffrement	Synchronisation	Idéal pour
<b>Bitwarden</b>	Cloud (ou auto-hébergement)	✓ Oui	AES-256	✓ Native (serveurs Bitwarden ou auto-hébergé)	Usage courant, multi-appareils, familles, débutants
<b>KeePass</b>	Local (fichier .kdbx)	✓ Oui	AES-256 / ChaCha20	✗ Manuelle (fichier à synchroniser)	Puristes, air-gapped, sécurité maximale, utilisateurs avancés
<b>Proton Pass</b>	Cloud (Proton)	✓ Oui	AES-256 (bout en bout)	✓ Native (serveurs Proton)	Déjà utilisateur Proton (Mail, Drive, VPN), écosystème intégré

**Note :** Les trois solutions sont **gratuites** en version de base, avec des options payantes pour des fonctionnalités supplémentaires (partage familial, stockage illimité, etc.).

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### 3. Comparatif détaillé

Critère	Bitwarden	KeePass	Proton Pass
<b>Prix (version gratuite)</b>	✓ Illimité (2 appareils)	✓ Illimité (aucune limite)	✓ Illimité (1 appareil ? à vérifier sur leur site)
<b>Applications mobiles officielles</b>	✓ iOS / Android	⚠ Tierces (KeePassDX, Strongbox)	✓ iOS / Android
<b>Extension navigateur</b>	✓ Oui	⚠ Tierce (KeePassXC-Browser)	✓ Oui
<b>Auto-hébergeable</b>	✓ Oui (Vaultwarden)	✓ Oui (fichier local)	✗ Non
<b>Nécessite un compte (email)</b>	✓ Oui	✗ Non	✓ Oui (compte Proton)
<b>Numéro de téléphone requis</b>	✗ Non	✗ Non	✗ Non
<b>Serveurs</b>	USA (mais open-source, auto-hébergeable)	Aucun (fichier local)	Suisse (Proton)
<b>Vérification de fuite de données</b>	✓ Oui (payant)	⚠ Tierce (HaveIBeenPwned)	✓ Oui (gratuit ? à vérifier)
<b>Partage de mots de passe</b>	✓ Oui (avec d'autres utilisateurs Bitwarden)	✗ Non (fichier partagé possible mais complexe)	✓ Oui (avec d'autres utilisateurs Proton)
<b>Générateur de mots de passe</b>	✓ Oui	✓ Oui	✓ Oui

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### 4. Comment choisir ? (Selon votre profil)

Si vous êtes...	Choisissez...	Pourquoi
<b>Débutant, usage quotidien, plusieurs appareils</b>	<b>Bitwarden</b>	Simple, gratuit, synchronisation automatique, communauté immense, extension navigateur intuitive.
<b>Exigeant / paranoïde, vous voulez le contrôle total</b>	<b>KeePass</b>	Fichier local, aucun serveur, aucune donnée transmise à qui que ce soit. Vous êtes le seul maître de vos secrets.
<b>Déjà utilisateur Proton (Mail, Drive, VPN)</b>	<b>Proton Pass</b>	Écosystème intégré, Suisse, pas de données supplémentaires à confier à une nouvelle entreprise.
<b>Vous voulez auto-héberger votre gestionnaire de mots de passe</b>	<b>Bitwarden (Vaultwarden)</b>	Léger, facile à déployer avec Docker, contrôle total sans dépendre des serveurs Bitwarden.
<b>Vous ne voulez absolument aucun compte en ligne</b>	<b>KeePass</b>	Zéro compte, zéro email, zéro cloud. Tout est sur votre disque dur ou clé USB.
<b>Vous cherchez la solution la plus simple et rapide à installer</b>	<b>Bitwarden</b> (gratuit, même pas de paiement)	Création de compte en 30 secondes, extension à installer, et c'est parti.
<b>Vous voulez du chiffré, mais sans la complexité de KeePass</b>	<b>Proton Pass</b>	Interface moderne, chiffré par défaut, et vous êtes déjà chez Proton.

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

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

#### Pourquoi Bitwarden ?

- **Simple** : extension navigateur + application mobile, tout se synchronise automatiquement.
- **Gratuit** : nombre illimité de mots de passe, 2 appareils (ordinateur + téléphone).
- **Open-source** : code auditable.
- **Auto-hébergeable** : via Vaultwarden (léger, compatible Docker).

#### Comment faire ? (Pas à pas)

##### Étape 1 : Créez un compte Bitwarden

1. Rendez-vous sur [bitwarden.com](https://bitwarden.com) → cliquez sur "Commencer" ou "Get Started".
2. **Créez un compte gratuit** (email, nom, mot de passe maître).
3. **Notez votre mot de passe maître** : c'est le seul mot de passe que vous devez retenir. Sans lui, impossible d'accéder à vos secrets. Conservez-le précieusement (papier + gestionnaire de mots de passe sécurisé).
4. Vérifiez votre adresse email.

##### Étape 2 : Installez Bitwarden sur vos appareils

Appareil	Action
<b>Ordinateur (navigateur)</b>	Installez l'extension Bitwarden (Chrome Web Store / Firefox Add-ons). Connectez-vous avec votre compte.
<b>Ordinateur (application)</b>	Téléchargez l'application de bureau (Windows/Mac/Linux) sur <a href="https://bitwarden.com/download">bitwarden.com/download</a> .
<b>Android</b>	Aurora Store (sans traçage) ou F-Droid → recherchez "Bitwarden".
<b>iPhone</b>	App Store → "Bitwarden" (Apple reste un tiers).

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### Installation sur Linux Mint (application de bureau)

Si vous préférez une application dédiée à l'extension navigateur :

#### Méthode 1 – Via Snap (recommandé, simple)

```
sudo apt update
sudo apt install snapd
sudo snap install bitwarden
```

#### Méthode 2 – Via AppImage (portable)

1. Rendez-vous sur [bitwarden.com/download](https://bitwarden.com/download) .
2. Téléchargez le fichier .AppImage pour Linux.
3. Ouvrez un terminal dans le dossier de téléchargement :

```
chmod +x Bitwarden-*.AppImage
./Bitwarden-*.AppImage
```

4. (Optionnel) Déplacez le fichier dans un dossier Applications et créez un raccourci manuellement.

#### Méthode 3 – Extension navigateur (la plus simple)

- Ouvrez Firefox (installé par défaut) ou Brave.
- Allez dans le menu « Extensions ».
- Recherchez « Bitwarden » et cliquez sur « Ajouter ».
- Connectez-vous avec votre compte (celui que vous avez créé sur [bitwarden.com](https://bitwarden.com) ).

💡 **Recommandation** : Pour les débutants, commencez par l'extension navigateur. Elle est identique à celle de Chrome/Windows et parfaitement fonctionnelle.

### Étape 3 : Importez vos mots de passe existants (depuis votre navigateur)

1. Dans le navigateur (Chrome/Edge/Firefox) : exportez vos mots de passe au format CSV (Paramètres → Mots de passe → Exporter).
2. Dans l'extension Bitwarden : Outils → Importer → choisissez le format (ex: "Chrome CSV").
3. Importez le fichier.
4. **Supprimez le fichier CSV** de votre disque dur (non chiffré).

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### Étape 4 : Changez vos mots de passe faibles

- 1.Bitwarden propose un **générateur de mot de passe** (intégré à l'extension).
- 2.Passez en revue vos mots de passe importés :
  - Supprimez les doublons
  - Changez les mots de passe faibles (longueur < 12 caractères, répétés)
  - Générez un mot de passe unique par site (exemple : xK9#mP2\$vL7\*QwR)

### Étape 5 (optionnel) : Auto-hébergement avec Vaultwarden (pour les plus techniques)

Prérequis : Docker sur un serveur (Raspberry Pi, VPS, vieux PC).

```
docker run -d --name vaultwarden \
  -e DOMAIN=https://votre-domaine.com \
  -e SIGNUPS_ALLOWED=false \
  -v /vw-data/:/data/ \
  -p 80:80 \
  vaultwarden/server:latest
```

Rendez-vous ensuite sur votre domaine pour créer votre compte. Ceci est pour des utilisateurs avancés.

### Limites de la version gratuite

- 2 appareils maximum (ex: 1 ordinateur + 1 mobile). Au-delà, il faut passer à la version payante (environ 10 \$/an).
- Pas de partage avec d'autres utilisateurs (payant).
- Pas de vérification de fuite de données (payant).

Pour la plupart des particuliers, la version gratuite est largement suffisante.

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### 6. Méthode B : KeePass (pour le contrôle total et l'absence de cloud)

#### Pourquoi KeePass ?

- **Zéro cloud** : votre base de mots de passe est un fichier local (extension `.kdbx`).
- **Zéro compte** : pas d'email, pas de serveur, pas de dépendance.
- **Sécurité maximale** : fichier chiffré (AES-256 ou ChaCha20). Personne n'y a accès si vous gardez votre mot de passe.
- **Open-source** et mature (plus de 20 ans d'existence).
- **Portable** : vous pouvez transporter votre base sur une clé USB.

#### Comment faire ? (Pas à pas)

##### Étape 1 : Installez KeePass sur votre ordinateur

Système	Action
Windows	Téléchargez KeePass ( <a href="https://keepass.info">keepass.info</a> ) → installez-le.
macOS	Utilisez <b>KeePassXC</b> (version multiplateforme) préférée.
Linux	<code>sudo apt install keepass2</code> (ou KeePassXC).

##### Étape 2 : Créez votre base de mots de passe (coffre-fort)

1. Lancez KeePass → "Nouvelle base de mots de passe" (New Database).
  2. **Choisissez un mot de passe maître TRÈS FORT** (phrase de passe de 5 mots aléatoires, ou 20 caractères).
- **Notez ce mot de passe** sur un papier stocké dans un endroit sécurisé (coffre, enveloppe fermée). Sans lui, votre base est perdue définitivement.
3. Choisissez l'emplacement du fichier `.kdbx` (ex: `Documents/keepass.kdbx`).
  4. (Optionnel) Ajoutez une **clé de fichier** (un fichier externe qui agit comme un second mot de passe). Cela renforce la sécurité, mais complexifie la restauration.

##### Étape 3 : Installez KeePass sur vos autres appareils

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

Appareil	Client recommandé
Android	KeePassDX (F-Droid) ou Keepass2Android
iPhone	Strongbox (gratuit avec limitation) ou KeePassium
Navigateur	KeePassXC-Browser (nécessite KeePassXC sur l'ordinateur)

### Étape 4 : Synchronisez votre fichier .kdbx entre appareils (optionnel)

La synchronisation est **manuelle** (c'est le prix du contrôle total). Plusieurs méthodes :

Méthode	Niveau
<b>Nextcloud</b> (voir fiche N°7)	Facile : déposez le fichier .kdbx dans votre dossier Nextcloud. Accédez-y depuis vos autres appareils avec l'application Nextcloud.
<b>Syncthing</b> (P2P)	Intermédiaire : synchronisation directe sans serveur.
<b>Clé USB manuelle</b>	Très simple : copiez le fichier sur une clé USB de temps en temps.

**⚠ Important** : Si vous synchronisez votre fichier via un cloud (Nextcloud), assurez-vous que le fichier .kdbx est bien **chiffré** (il l'est par KeePass avant de quitter votre ordinateur). Ce n'est pas un problème, même si Nextcloud est piraté.

### Étape 5 : Importez vos mots de passe (depuis votre navigateur)

1. Exportez vos mots de passe depuis votre navigateur (CSV).
2. Dans KeePass/XC : "Importer" → choisissez le format (CSV).
3. **Supprimez le fichier CSV** non chiffré.

### Astuce KeePass : générez des mots de passe robustes

- Dans KeePass, ouvrez le générateur de mot de passe (icône clé).
- Paramètres recommandés : longueur 16-20 caractères, tous types de caractères.
- Copiez directement dans l'interface.

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### Limites de KeePass

- Pas de synchronisation automatique (à gérer manuellement). Ce n'est pas un problème pour certains, mais cela peut rebuter les débutants.
- Pas de "remplissage automatique" aussi intégré que Bitwarden (mais possible via extensions tierces).
- Interface moins moderne, surtout sur Windows (KeePass original). KeePassXC est plus agréable.

Pour qui ? Utilisateurs avancés, paranoïdes, personnes qui ne veulent absolument aucun cloud, ou qui ont déjà une solution de synchronisation (Nextcloud, Syncthing).

## 7. Méthode C : Proton Pass (écosystème intégré pour les utilisateurs Proton)

### Pourquoi Proton Pass ?

- **Ancré dans l'écosystème Proton** : si vous avez déjà Proton Mail, Proton Drive, Proton VPN, Proton Pass s'intègre naturellement.
- **Chiffré de bout en bout** comme le reste des services Proton.
- **Serveurs en Suisse** (hors UE mais législation protectrice).
- **Interface moderne** et applications mobiles réussies.
- **Pas de numéro de téléphone.**

### Comment faire ? (Pas à pas)

#### Étape 1 : Créez un compte Proton (si ce n'est pas déjà fait)

1. Rendez-vous sur [proton.me](https://proton.me).
2. Créez un compte gratuit (email, mot de passe). **Notez vos codes de récupération** imprimés.

#### Étape 2 : Activez Proton Pass

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

- Connectez-vous à votre compte Proton.
- Dans le tableau de bord, cliquez sur "Proton Pass" ou allez sur [pass.proton.me](https://pass.proton.me).
- Activez le service (gratuit).

### Étape 3 : Installez Proton Pass sur vos appareils

Appareil	Action
Ordinateur (navigateur)	Extension Chrome/Firefox : recherchez "Proton Pass".
Ordinateur (application)	Application de bureau (Windows/Mac) disponible sur <a href="https://proton.me/download">proton.me/download</a> .
Android	Aurora Store → "Proton Pass".
iPhone	App Store → "Proton Pass".

### Étape 4 : Importez vos mots de passe

- Dans l'extension ou l'application : Outils → Importer.
- Choisissez votre navigateur (Chrome, Edge, Firefox) ou un fichier CSV.
- L'importation se fait en local, chiffrée avant envoi.

### Étape 5 : Générez des alias email (optionnel mais puissant)

Proton Pass permet de créer des **alias email** (ex: [amazon.123@passmail.net](mailto:amazon.123@passmail.net)) pour chaque site, afin de ne pas donner votre adresse réelle. Utile pour les inscriptions.

### Limites de la version gratuite

- Nombre limité d'alias (à vérifier sur leur grille tarifaire).
- Nombre limité d'appareils (1 appareil dans la version gratuite selon les conditions actuelles).
- Certaines fonctionnalités (vérification de fuite de données, 2FA intégrée) sont payantes.

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

Proton Pass est idéal si vous **êtes déjà dans l'écosystème Proton**. Sinon, Bitwarden ou KeePass sont plus simples/plus puissants.

### 8. Tableau récapitulatif des fonctionnalités (gratuit vs payant)

Fonctionnalité	Bitwarden (gratuit)	Bitwarden (payant ~10\$/an)	KeePass (gratuit)	Proton Pass (gratuit)	Proton Pass (payant)
Mots de passe illimités	✓	✓	✓	✓	✓
Appareils simultanés	2	illimités	illimités	1 (?)	illimités
Extension navigateur	✓	✓	⚠ (KeePassXC)	✓	✓
Vérification de fuite	✗	✓	✗ (tierce)	✗	✓
Partage avec d'autres	✗	✓	✗	✗	✓
Auto-hébergement	✓	✓	✓	✗	✗
Alias email	✗	✓	✗	✓ (limité)	✓


### 9. Cas particulier : KeePass et la synchronisation

La critique la plus fréquente de KeePass est l'absence de synchronisation automatique. Voici comment la **résoudre simplement** :

Méthode	Niveau de difficulté	Compatibilité
Déposer le fichier <code>.kdbx</code> dans un dossier Nextcloud (voir fiche N°7)	Facile	Ordinateur + mobile (via Nextcloud)
Utiliser Syncthing (P2P)	Intermédiaire	Tous appareils (synchronisation)

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

Méthode	Niveau de difficulté	Compatibilité
		directe)
Conserver sur clé USB et copier manuellement	Très simple	Pas de synchronisation automatique
Utiliser un outil comme FreeFileSync	Facile	Synchronisation programmée avec disque externe

 **Recommandation pour les débutants KeePass** : Utilisez Nextcloud (gratuit, 2 Go avec [Frama.space](https://framap.space) ). Déposez votre fichier `.kdbx` dedans. Depuis votre mobile, accédez-y via l'application Nextcloud + KeePassDX. Cela ajoute un cloud, mais le fichier reste chiffré par KeePass.

### 10. À savoir avant de se lancer

Crainte fréquente	La réalité
"Je vais perdre tous mes mots de passe si j'oublie mon mot de passe maître."	C'est vrai pour <b>tous les gestionnaires</b> . C'est LE risque. Sauvegardez votre mot de passe maître sur un papier dans un endroit sécurisé (coffre, enveloppe scellée).
"Bitwarden est américain, je ne lui fais pas confiance."	Bitwarden est open-source, vous pouvez <b>auto-héberger</b> votre instance (Vaultwarden). Ou choisissez KeePass (aucun cloud) ou Proton Pass (Suisse).
"KeePass a l'air compliqué, je n'ose pas."	Il existe une version simplifiée : <b>KeePassXC</b> (plus moderne). Commencez par Bitwarden si KeePass vous semble difficile.
"Est-ce que je peux utiliser plusieurs gestionnaires en même temps ?"	Oui, mais déconseillé (risque de désynchronisation). Préférez un seul gestionnaire.
"Et si je veux partager des mots de passe avec ma famille ?"	Bitwarden (payant) le permet. Proton Pass (payant) aussi. KeePass non (sauf fichier partagé, mais peu pratique).

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

### 11. Challenge 7 jours

**Challenge** : Pendant 7 jours, utilisez votre nouveau gestionnaire de mots de passe **exclusivement**. Ne remplissez plus jamais un mot de passe manuellement.

#### À faire :

1. Installez Bitwarden / KeePass / Proton Pass.
2. Importez vos mots de passe existants.
3. À chaque nouvelle inscription, utilisez le **générateur de mot de passe intégré**.
4. Supprimez les mots de passe enregistrés dans votre navigateur (Chrome/Edge/Safari).

#### Vous allez constater :

- Vous ne "tapez" plus jamais un mot de passe (sauf le maître).
- Les générateurs produisent des mots de passe bien plus forts que les vôtres.
- Vous pouvez avoir un mot de passe **unique** par site, sans vous en souvenir.

**Après 7 jours**, vous ne pourrez plus vous en passer.

### 12. Alternatives et approfondissements

Si vous avez besoin de...	Essayez plutôt...
Une solution 100 % hors ligne et portable (clé USB)	<b>KeePass</b> avec clé USB chiffrée (VeraCrypt)
Une solution pour toute la famille (partage)	<b>Bitwarden</b> (payant) ou <b>Proton Pass</b> (payant)
Auto-héberger votre gestionnaire (contrôle total)	<b>Vaultwarden</b> (Bitwarden) ou <b>KeePass</b> (fichier)
Une solution pour entreprises	<b>Bitwarden</b> (Business) ou <b>KeePass</b> (si petites équipes tech)

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

Si vous avez besoin de...	Essayez plutôt...
Une extension navigateur la plus simple possible	<b>Bitwarden</b> ou <b>Proton Pass</b> (KeePass nécessite KeePassXC-Bridge)

### 13. En résumé (ce que vous gagnez)

Action	Bénéfice
Utiliser <b>Bitwarden</b>	Gestionnaire cloud simple, gratuit, open-source, synchronisé, idéal pour débutants et multi-appareils
Utiliser <b>KeePass</b>	Contrôle total, zéro cloud, zéro compte, fichier local chiffré – sécurité maximale
Utiliser <b>Proton Pass</b>	Intégré à l'écosystème Proton (Suisse), moderne et chiffré par défaut
Quitter le gestionnaire de votre navigateur	Plus de stockage de vos mots de passe sur les serveurs big tech (Google, Microsoft, Apple)
Utiliser un mot de passe unique par site	Un site piraté ne compromet pas tous vos autres comptes
Utiliser le générateur intégré	Des mots de passe longs, aléatoires, impossible à deviner

### Conclusion générale

Si vous êtes...	Choisissez...
<b>Débutant / usage quotidien / plusieurs appareils</b>	<b>Bitwarden</b> (gratuit, simple, fiable)
<b>Exigeant / paranoïde / pas de cloud</b>	<b>KeePass</b> (fichier local, zéro serveur)
<b>Déjà utilisateur Proton (Mail, Drive, VPN)</b>	<b>Proton Pass</b> (écosystème intégré)
<b>Vous voulez auto-héberger</b>	<b>Bitwarden</b> (Vaultwarden)
<b>Vous ne voulez aucun compte en ligne</b>	<b>KeePass</b>

À retenir absolument :

## Fiche Pratique N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass (libre et sans big tech) V1.1

- **Votre mot de passe maître est la clé de tous vos secrets.** Perdez-le → perdez tous vos comptes.
- Sauvegardez-le sur un **support papier** (coffre, enveloppe scellée). Ne le stockez pas en ligne non chiffré.
- Utilisez un **mot de passe unique par site** – c'est la règle d'or de la sécurité numérique.
- N'importe laquelle de ces trois solutions est **infiniment meilleure** que le gestionnaire de votre navigateur ou que la réutilisation du même mot de passe partout.

### Test final :

- Créez un compte sur un site factice (ou un vrai) avec un mot de passe généré par votre gestionnaire.
- Déconnectez-vous.
- Utilisez le remplissage automatique pour vous reconnecter.
- Si cela a fonctionné : **vous avez réussi** ✓