Bitwarden

SOMMAIRE

1. Qu’est-ce que Bitwarden

Bitwarden est un gestionnaire de mots de passe pour **stocker**, **gérer** et **partager** de manière **sécurisée** des **données** en ligne **sensibles** telles que les mots de passe, les clés de passe et les cartes de paiement.

La problématique à l’origine de l’installation de Bitwarden est celle liée à l’**authentification** des collaborateurs sur les services web utilisés au sein de DELIVAGRI.

Exemple: Google Drive, Ringover, etc.

bitwarden

L’installation de Bitwarden a pour but de **faciliter l’authentification** des utilisateurs et d’**accroître le niveau de sécurisation** des accès aux données de l’entreprise

3. Rappel sur les mots de passe

1. Utilisez un mot de passe différent pour chaque service :

En cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient **piratables**.

2. Utilisez un mot de passe suffisamment long et complexe :

Une attaque par « force brute », consistant à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe, réalisées par des ordinateurs, permettant de tester des dizaines de milliers de combinaisons par seconde.

Un bon mot de passe doit comporter au minimum **12 caractères** mélangeant des **majuscules**, des **minuscules**, des **chiffres** et des **caractères spéciaux**.

3. Rappel sur les mots de passe

3. Utilisez un mot de passe impossible à deviner :

Une attaque par « dictionnaire » consistant à deviner le mot de passe.

Évitez d'employer dans vos mots de passe des **informations personnelles** facilement accessibles sur le web, comme le prénom de votre enfant, une date anniversaire, votre groupe de musique préféré, le nom de l'entreprise, etc.

Évitez les **suites logiques simples** comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons tester par les cybercriminels.

3. Rappel sur les mots de passe

4. Utilisez un gestionnaire de mots de passe (Bitwarden) :

Il est impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement.

Ne commettez pas pour autant l'erreur de les **noter sur un pense-bête** que vous laisseriez à **proximité de votre équipement**, ni de les **inscrire dans votre messagerie** ou dans un **fichier non protégé** de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès.

Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le **seul mot de passe** qui permet d'en ouvrir l'accès.

3. Rappel sur les mots de passe

5. Changez votre mot de passe au moindre soupçon

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

6. Ne communiquez jamais vos mots de passe à un tiers

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

3. Rappel sur les mots de passe

7. N’utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel.

Si vous êtes obligé d’utiliser un ordinateur partagé, utilisez le mode de « navigation privée » du navigateur, qui permet d’éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et **n’enregistrez jamais vos mots de passe dans le navigateur**.

Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l’ordinateur partagé.

3. Rappel sur les mots de passe

8. Activez la « double authentification » lorsque c’est possible

Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option.

En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique.

Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. Pour en savoir plus, retrouvez notre article sur la double authentification.

3. Rappel sur les mots de passe

9. Changez les mots de passe par défaut des différents services auxquels vous accédez

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels.

Aussi, il est important de les **remplacer au plus vite par vos propres mots de passe** que vous contrôlez.

3. Rappel sur les mots de passe

10. Choisissez un mot de passe particulièrement robuste pour votre messagerie

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes.

Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.
Votre mot de passe de messagerie est donc l'un des plus importants à protéger.

4. Intérêt de Bitwarden

Bitwarden répond aux exigences des points 1, 2, 3, 4 et 10.

Un unique mot de passe à retenir pour accéder au coffre fort contenant l'intégralité des mots de passe robuste utilisés.

Il assure que le site web auquel vous accédez et bien authentique.

Petit plus : L'abonnement famille pour pouvoir sécuriser vos mots de passe sur vos équipements personnels.

5. Première connexion à Bitwarden

Pour votre 1ère connexion,

vous recevrez un mail de :

noreply@bitwarden.eu

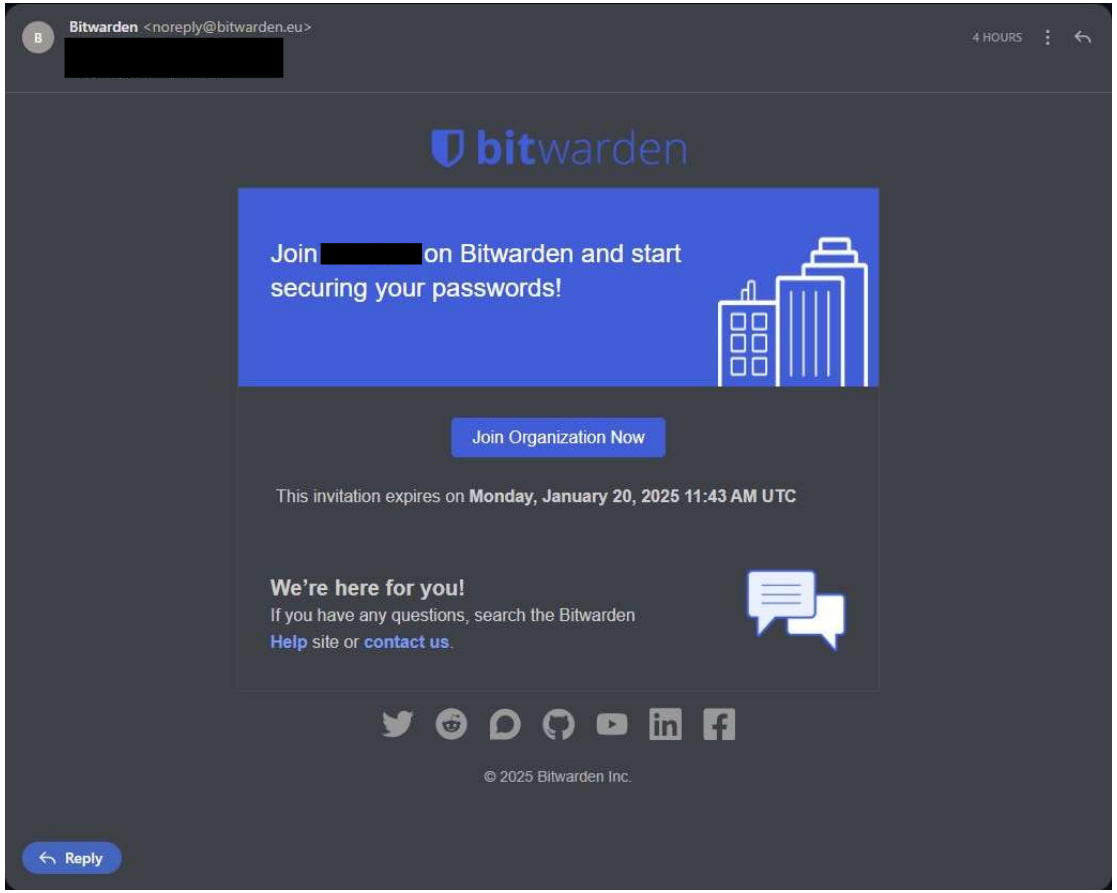
Cliquez sur :

Join Organization Now

Puis renseignez les éléments demandés.

Après validation, vous aurez accès

au **Coffre (Vault) de DELIVAGRI**.



6. Intégration de Bitwarden dans Chrome

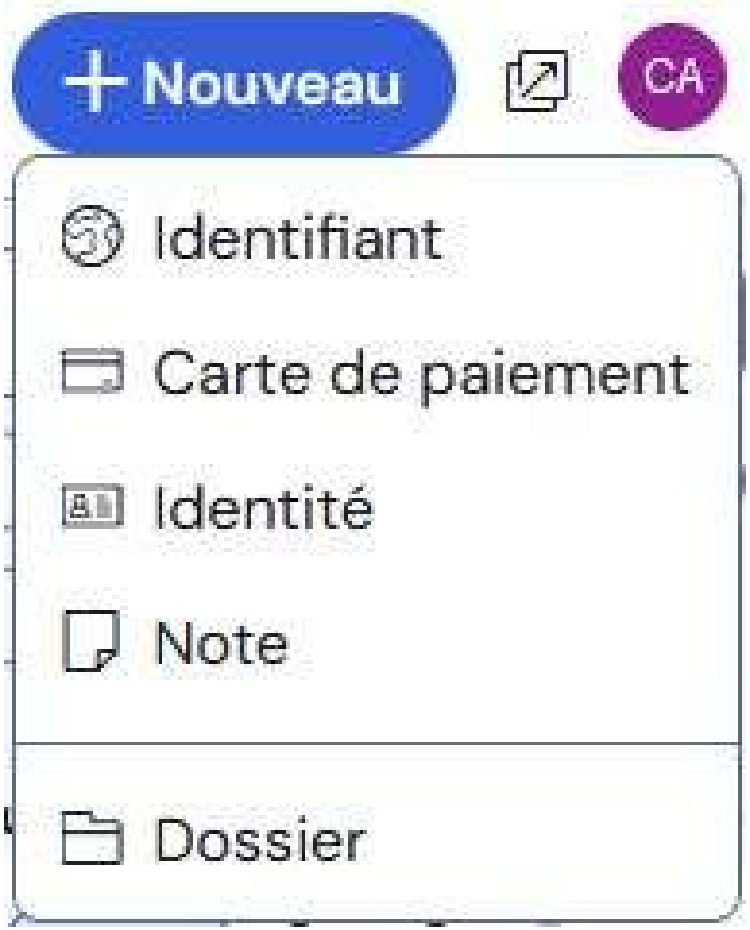
Dans le coin supérieur droit de votre navigateur Chrome, vous trouverez le logo de Bitwarden

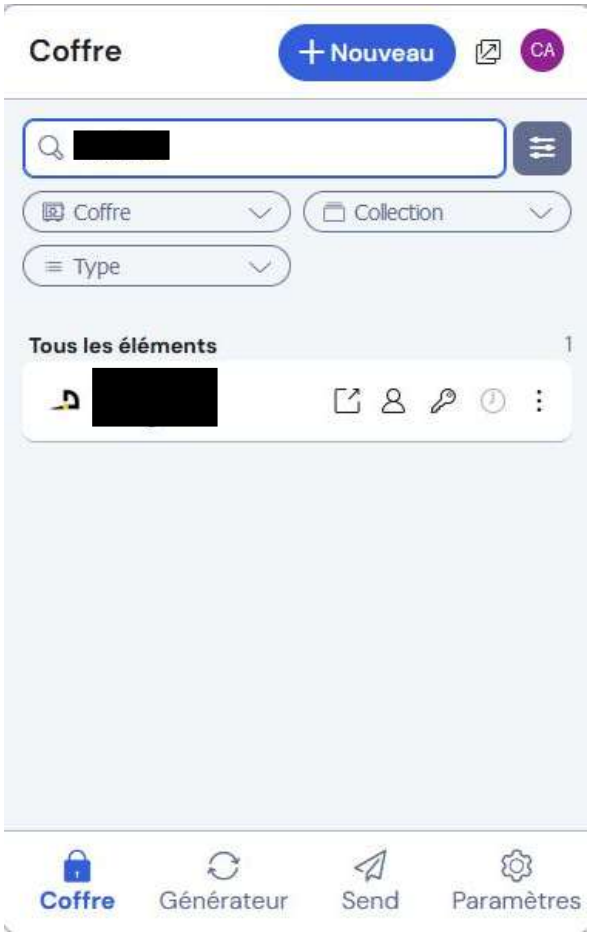
Une fois authentifié, vous avez accès à Bitwarden qui vous permet de :

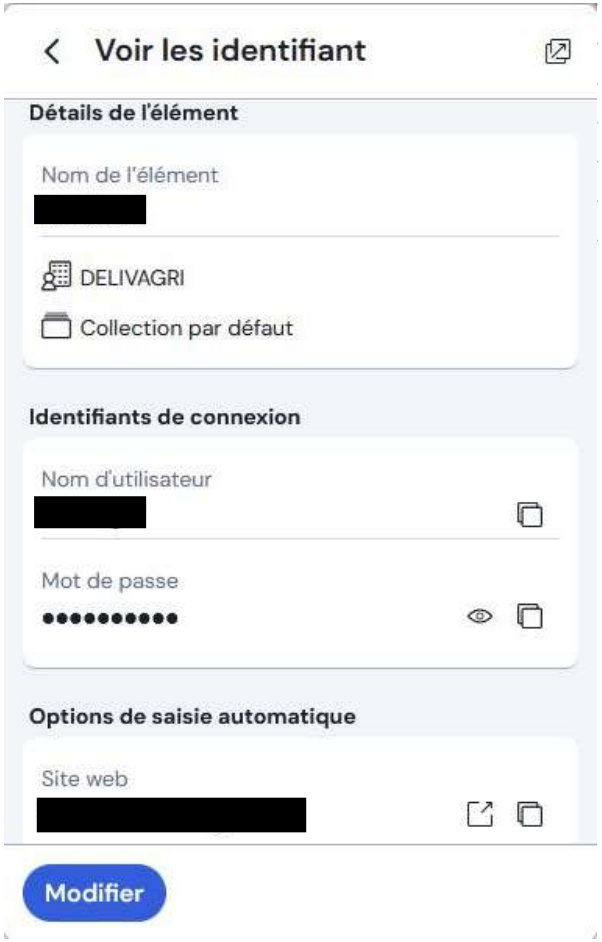
- créer des mots de passe 

- accéder au site web 
- copier l'identifiant 
- copier le mot de passe 

6. Intégration de Bitwarden dans Chrome







6. Intégration de Bitwarden dans Chrome

Concernant le **remplissage de l'identifiant et du mot de passe** sur la page web désiré :

- Possibilité de configurer l'auto-remplissage :

  Paramètres > Saisie Automatique > Cochez "Saisir automatiquement au chargement de la page".

- Possibilité de remplir manuellement :

  Raccourci **ctrl + maj + L**

Avez-vous des questions?