MON COMPTE > SE CONNECTER & DÉVERROUILLER

Protection de l'ouverture de session pour les nouveaux appareils (février/mars 2025)

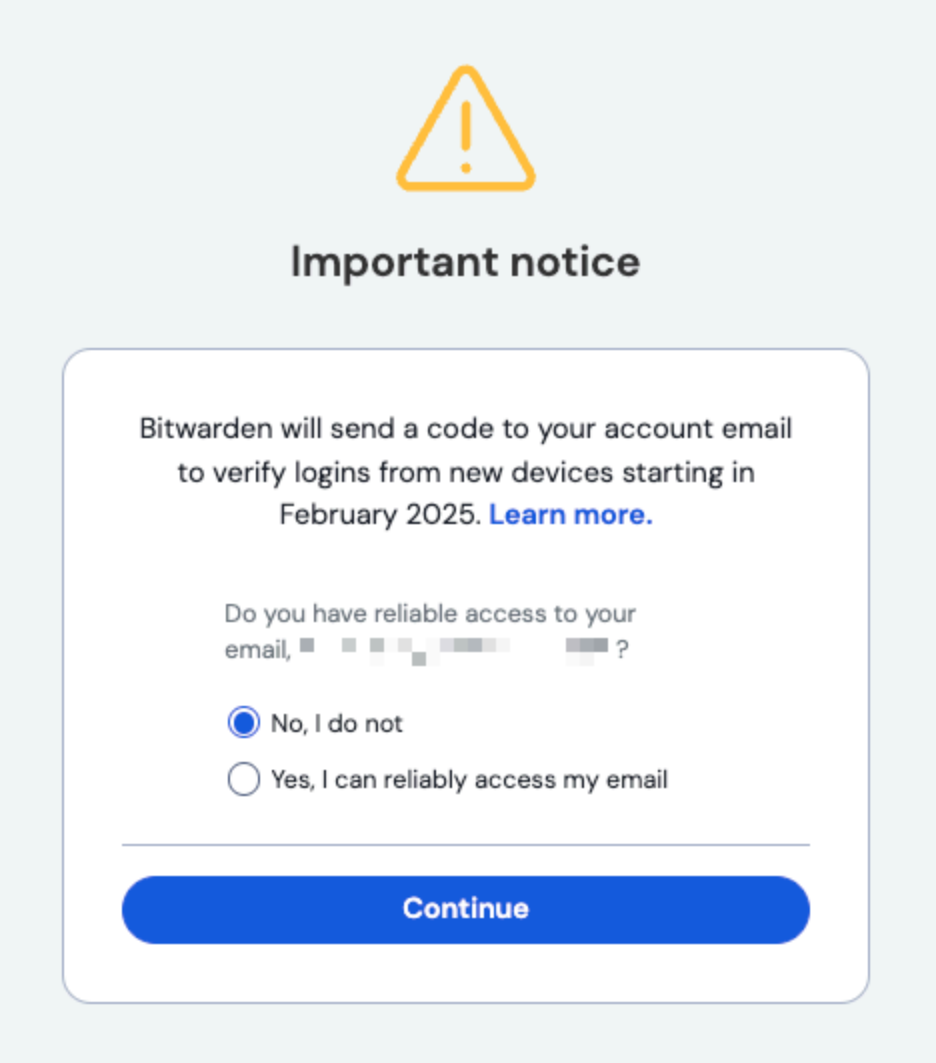
Protection de l'ouverture de session pour les nouveaux appareils (février/mars 2025)

Pour assurer la sécurité de votre compte, à partir de février/mars 2025, Bitwarden exigera une vérification supplémentaire **pour les utilisateurs qui n'utilisent pas la connexion** en deux étapes. Après avoir saisi votre mot de passe principal Bitwarden, vous serez invité à saisir un code de vérification à usage unique envoyé à l'adresse électronique de votre compte afin de compléter le processus de connexion **lorsque vous vous connectez à partir d'un appareil sur lequel vous ne vous êtes pas connecté auparavant**. Par exemple, si vous vous connectez à une application mobile ou à une extension de navigateur que vous avez déjà utilisée, vous ne recevrez pas cette invitation.

La plupart des utilisateurs ne verront pas cette invite, à moins qu'ils ne se connectent fréquemment à de nouveaux appareils. Cette vérification n'est nécessaire que pour les nouveaux appareils ou après avoir effacé les cookies du navigateur.

Si vous accédez régulièrement à votre courrier électronique, la récupération du code de vérification devrait être simple. Si vous préférez ne pas vous fier à l'email de votre compte Bitwarden pour la vérification, vous pouvez configurer la connexion en deux étapes via une application Authenticator, une clé matérielle, ou la connexion en deux étapes via un email différent.

Les utilisateurs concernés par ce changement verront la communication suivante dans le produit et devraient avoir reçu un courriel les informant du changement :



Annonce de la vérification d'un nouveau dispositif

FAQ

Quand cela se produira-t-il ?

Ce changement entrera en vigueur à partir de février/mars 2025. Cette page sera mise à jour dès qu'une date aura été fixée pour la publication.

Pourquoi Bitwarden met-il cela en œuvre ?

Bitwarden met en œuvre ce changement pour améliorer la sécurité des utilisateurs qui n'ont pas activé la connexion en deux étapes. Si quelqu'un accède à votre mot de passe, il ne pourra toujours pas se connecter à votre compte sans vérification secondaire (le code envoyé à votre courrier électronique). Cette couche supplémentaire permet de protéger vos données contre les pirates informatiques qui ciblent souvent les mots de passe faibles ou exposés pour obtenir un accès non autorisé.

Quand serai-je invité à procéder à cette vérification ?

Cette vérification ne vous sera demandée que lorsque vous vous connecterez à partir de nouveaux appareils. Si vous vous connectez à un appareil que vous avez déjà utilisé, vous ne serez pas invité à le faire.

Qu'est-ce qui est considéré comme un nouveau dispositif ?

Un nouvel appareil est un appareil qui n'a pas été utilisé auparavant pour se connecter à votre compte Bitwarden. Il peut s'agir d'un nouveau téléphone, d'une nouvelle tablette, d'un nouvel ordinateur ou d'une extension de navigateur à partir de laquelle vous ne vous êtes jamais connecté. Lorsque vous vous connectez à partir d'un nouvel appareil, il vous est demandé de vérifier votre identité à l'aide d'un code à usage unique envoyé à votre adresse électronique.

D'autres scénarios qui déclencheront la création d'un nouveau dispositif sont les suivants :

- La désinstallation et la réinstallation de l'application mobile, de l'application pour ordinateur de bureau ou de l'extension de navigateur entraîneront la création d'un nouveau dispositif.
- L'effacement des cookies du navigateur lancera un nouvel appareil pour l'application web, mais pas pour les extensions du navigateur.

Mes identifiants de messagerie sont enregistrés dans Bitwarden. Serai-je bloqué hors de Bitwarden ?

Les codes de vérification par courriel ne seront exigés sur les nouveaux appareils que pour les utilisateurs dont la connexion en deux étapes n'est pas activée. Vous ne verrez pas cette invite sur les appareils déjà connectés et vous vous connecterez normalement avec l'adresse électronique de votre compte et votre mot de passe principal.

Si vous vous connectez à un nouvel appareil, l'email de votre compte Bitwarden recevra un code de vérification à usage unique. Si vous avez accès à votre courriel, c'est-à-dire à un courriel de connexion persistant sur votre téléphone portable, vous pourrez saisir le code de vérification à usage unique pour vous connecter. Une fois connecté au nouvel appareil, le code de vérification ne vous sera plus demandé.

Si vous vous connectez régulièrement à votre messagerie en utilisant les informations d'identification enregistrées dans Bitwarden ou si vous ne voulez pas vous fier à votre messagerie pour la vérification, vous devez mettre en place une connexion en deux étapes qui sera indépendante de la messagerie du compte Bitwarden. Il peut s'agir d'une application d'authentification, d'une clé de sécurité ou d'une connexion en deux étapes par courriel avec un autre courriel. Si l'une des méthodes 2FA est activée, l'utilisateur n'est pas autorisé à vérifier le nouvel appareil par courrier électronique. Les utilisateurs dont la fonction 2FA est activée doivent également conserver leur code de récupération Bitwarden dans un endroit sûr.

Qui est exclu de la vérification des nouveaux dispositifs par courriel ?

Les catégories de connexions suivantes sont exclues :

- Les utilisateurs dont la connexion en deux étapes est configurée sont exclus.

- Les utilisateurs qui se connectent avec SSO, une clé d'accès ou une clé API sont exclus.
- Les utilisateurs auto-hébergés sont exclus.
- Les utilisateurs qui se connectent à partir d'un appareil où ils se sont déjà connectés sont exclus.
- Les utilisateurs qui se désinscrivent à partir de l'écran **Paramètres → Mon compte** sont exclus (**non recommandé**).

Mon organisation utilise le SSO, mes utilisateurs doivent-ils procéder à une vérification des nouveaux appareils ?

Non. Les utilisateurs qui se connectent avec SSO seront exemptés et ne seront pas invités à vérifier leur connexion sur un nouvel appareil. Toutefois, si un utilisateur, sans que la connexion en deux étapes soit activée, se connecte avec un nom d'utilisateur et un mot de passe sans passer par le SSO, il lui sera demandé de vérifier le nouvel appareil.

Je ne veux pas partager mon véritable email avec Bitwarden, comment puis-je configurer mon compte ?

Les utilisateurs qui souhaitent rester anonymes disposent de plusieurs options :

- Utilisez une option de connexion en deux étapes qui ne nécessite pas d'email, y compris une application d'authentification, une clé de sécurité ou une connexion en deux étapes par email avec un email différent.
- Utilisez un service de transfert d'alias de courrier électronique.
- Bitwarden auto-hébergé.

Bitwarden encourage les utilisateurs à avoir une adresse électronique active, car Bitwarden envoie des alertes de sécurité importantes comme les tentatives de connexion échouées.

Si j'utilise le code de récupération 2FA sur un nouvel appareil parce que j'ai perdu mon accès 2FA, serai-je toujours soumis à la vérification du nouvel appareil ?

Bitwarden va mettre à jour le flux du code de récupération de sorte que lorsque vous soumettez votre mot de passe et votre code de récupération, vous êtes connecté à l'application web et vous accédez à vos paramètres 2FA. Si vous craignez d'être bloqué, **évitez** de suivre cette procédure dans un navigateur incognito ou sur un appareil dont la connectivité internet n'est pas fiable, afin de vous assurer que vous pouvez effectuer toutes les étapes de configuration nécessaires au cours de cette session connectée.

Je veux me retirer ! Existe-t-il une option pour ?

Il s'agit d'une sécurité supplémentaire pour les utilisateurs dont la connexion en deux étapes n'est pas activée. Les utilisateurs qui n'ont pas activé la connexion en deux étapes sont plus vulnérables aux accès non autorisés par des pirates, car les mots de passe peuvent être compromis de multiples façons, même s'ils sont forts et uniques. Par exemple, les méthodes les plus courantes sont les suivantes

- Les attaques de phishing : Les cybercriminels utilisent des courriels ou des sites web trompeurs pour vous inciter à révéler votre mot de passe.
- Ingénierie sociale : Les attaquants peuvent tenter de vous manipuler ou de vous tromper pour que vous révéliez votre mot de passe par le biais d'appels téléphoniques, de textos ou d'autres moyens.
- Craquage de **mot de passe par des attaques** par force brute : Les attaquants utilisent des outils automatisés pour tenter à plusieurs reprises de deviner le mot de passe.
- **Enregistreur de frappe ou logiciel malveillant** : si votre appareil est infecté par un logiciel malveillant ou un enregistreur de frappe, les pirates peuvent enregistrer toutes les frappes que vous effectuez, y compris votre mot de passe, sans que vous le sachiez.

Avec la nouvelle vérification des appareils, même si votre mot de passe est compromis par l'une des méthodes ci-dessus, l'attaquant devra toujours récupérer la deuxième vérification, c'est-à-dire le code à usage unique contenu dans votre courrier électronique. Cela réduit considérablement la probabilité d'un accès non autorisé.

La nouvelle vérification de l'appareil est conçue pour être moins intrusive que la connexion traditionnelle en deux étapes. Elle ne s'applique que lorsque vous vous connectez à partir d'un appareil ou d'un client que vous n'avez jamais utilisé auparavant, de sorte que la plupart des utilisateurs ne subiront pas cette étape supplémentaire, puisqu'ils se connectent régulièrement à partir de leurs appareils habituels. Le processus de vérification utilise votre adresse électronique, que de nombreuses personnes gardent ouverte sur leur téléphone ou leur ordinateur, de sorte que la récupération du code est rapide et facile.

Les utilisateurs qui peuvent rencontrer des difficultés sont ceux qui font ce qui suit :

- La connexion en deux étapes n'est pas activée.
- Stocker le mot de passe de leur courrier électronique dans Bitwarden.
- Désinstaller et réinstaller constamment Bitwarden.
- Se déconnecter de leur messagerie électronique partout.

Seuls les utilisateurs qui font toutes ces choses et qui remplissent les conditions ci-dessus connaîtront des problèmes avec cette mise à jour de sécurité. Si les utilisateurs se retrouvent bloqués hors de leur compte, ils peuvent contacter le service Customer Success de Bitwarden.

Si les utilisateurs ne souhaitent pas la vérification des nouveaux appareils, il est fortement recommandé d'activer une autre méthode de connexion en deux étapes (soit via une application d'authentification, une clé matérielle ou un autre courrier) pour protéger votre compte.

Si les utilisateurs ne veulent pas de vérification des nouveaux appareils, ne veulent pas mettre en place une autre méthode de connexion en deux étapes et **ne veulent pas de sécurité sur leur compte,** ils peuvent choisir de ne pas le faire en accédant à l'écran **Paramètres → Mon compte** et en faisant défiler la page jusqu'à la section Zone de danger. Nous devons insister sur le fait que cette pratique est **fortement déconseillée**, car elle rend votre compte vulnérable à diverses attaques.