MI CUENTA > INICIAR SESIÓN & DESBLOQUEAR

Protección de inicio de sesión de nuevos dispositivos (febrero / marzo de 2025)

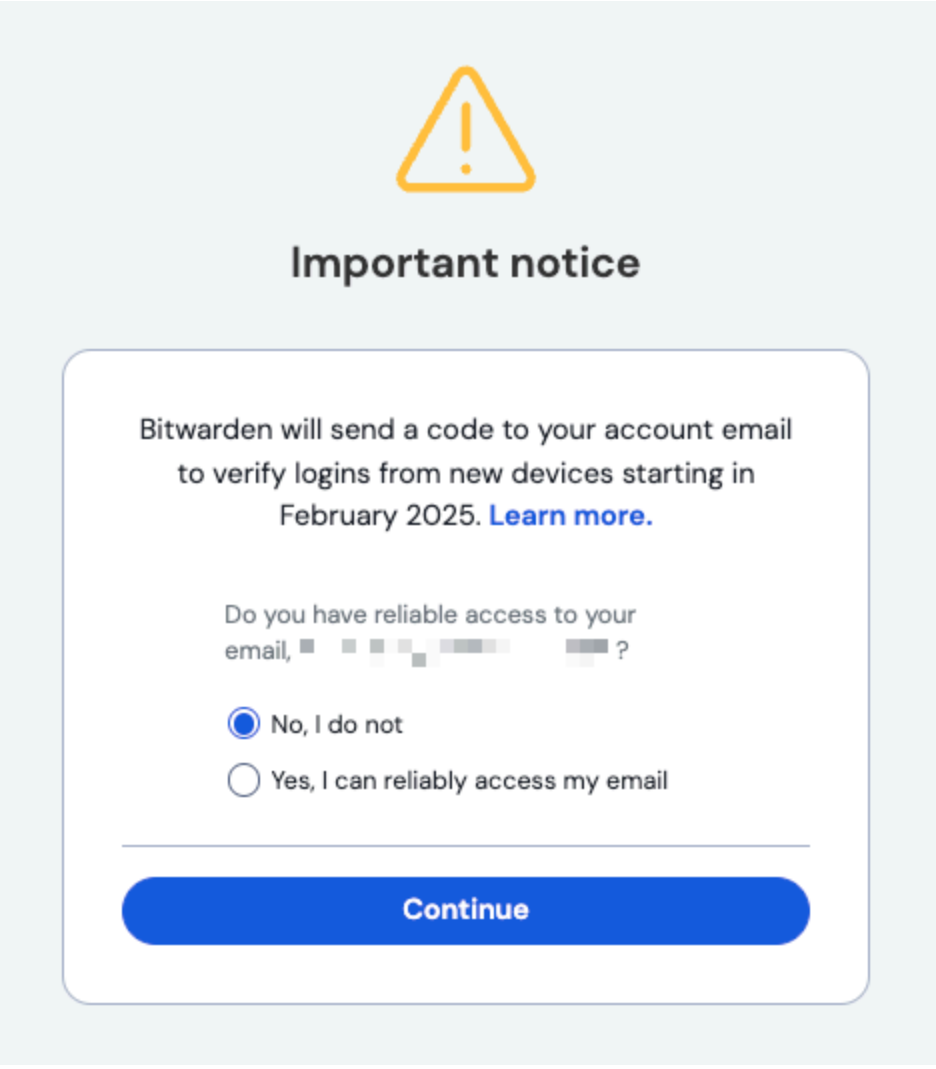
Protección de inicio de sesión de nuevos dispositivos (febrero / marzo de 2025)

Para mantener su cuenta segura, a partir de febrero / marzo de 2025, Bitwarden requerirá una verificación adicional **para los usuarios que no utilicen el inicio de sesión** en dos pasos. Después de introducir su contraseña maestra de Bitwarden, se le pedirá que introduzca un código de verificación de un solo uso enviado al correo electrónico de su cuenta para completar el proceso de inicio de sesión **cuando inicie sesión desde un dispositivo en el que no haya iniciado sesión anteriormente**. Por ejemplo, si está iniciando sesión en una aplicación móvil o en una extensión del navegador que ya ha utilizado anteriormente, no recibirá esta indicación.

La mayoría de los usuarios no experimentarán este aviso a menos que inicien sesión con frecuencia en nuevos dispositivos. Esta verificación sólo es necesaria para dispositivos nuevos o después de borrar las cookies del navegador.

Si accedes regularmente a tu correo electrónico, recuperar el código de verificación debería ser sencillo. Si prefieres no depender del correo electrónico de tu cuenta de Bitwarden para la verificación, puedes configurar el inicio de sesión en dos pasos a través de una aplicación Authenticator, una llave hardware o el inicio de sesión en dos pasos a través de un correo electrónico diferente.

Los usuarios afectados por este cambio verán la siguiente comunicación en el producto y deberían haber recibido un correo electrónico informándoles del cambio:



Anuncio de verificación de nuevos dispositivos

Preguntas frecuentes

¿Cuándo ocurrirá esto?

Este cambio entrará en vigor en febrero o marzo de 2025. Esta página se actualizará cuando se haya definido una fecha para el lanzamiento.

¿Por qué lo aplica Bitwarden?

Bitwarden está implementando este cambio para mejorar la seguridad de los usuarios que no tienen activado el inicio de sesión en dos pasos. Si alguien consigue acceder a tu contraseña, no podrá entrar en tu cuenta sin una verificación secundaria (el código enviado a tu correo electrónico). Esta capa adicional ayuda a proteger sus datos de los piratas informáticos, que a menudo utilizan contraseñas débiles o expuestas para obtener acceso no autorizado.

¿Cuándo se me solicitará esta verificación?

Sólo se le pedirá esta verificación cuando inicie sesión desde dispositivos nuevos. Si vas a iniciar sesión en un dispositivo que ya has utilizado antes, no se te pedirá que lo hagas.

¿Qué se considera un nuevo dispositivo?

Un dispositivo nuevo es cualquier dispositivo que no haya sido utilizado previamente para iniciar sesión en su cuenta de Bitwarden. Puede tratarse de un nuevo teléfono, tableta, ordenador o extensión del navegador desde el que nunca te hayas conectado. Cuando inicies sesión desde un nuevo dispositivo, se te pedirá que verifiques tu identidad mediante un código de un solo uso enviado a tu correo electrónico.

Otros escenarios que iniciarán un nuevo dispositivo serán:

- Al desinstalar y volver a instalar la aplicación móvil o de escritorio, o la extensión del navegador, se iniciará un nuevo dispositivo.
- Borrar las cookies del navegador iniciará un nuevo dispositivo para la aplicación web, pero no para las extensiones del navegador.

Mis credenciales de correo electrónico se guardan en Bitwarden. ¿Me quedaré fuera de Bitwarden?

Los códigos de verificación por correo electrónico sólo serán necesarios en los nuevos dispositivos para los usuarios que no tengan activado el inicio de sesión en dos pasos. Este mensaje no aparecerá en los dispositivos en los que se haya iniciado sesión previamente, sino que se iniciará la sesión normalmente con la dirección de correo electrónico de la cuenta y la contraseña maestra.

Si está iniciando sesión en un nuevo dispositivo, el correo electrónico de su cuenta Bitwarden recibirá un código de verificación de un solo uso. Si tiene acceso a su correo electrónico, es decir, un correo electrónico de inicio de sesión persistente en su teléfono móvil, podrá obtener el código de verificación de un solo uso para iniciar sesión. Una vez iniciada la sesión en el nuevo dispositivo, no se te volverá a pedir el código de verificación.

Si inicia sesión regularmente en su correo electrónico utilizando credenciales guardadas en Bitwarden o no desea depender de su correo electrónico para la verificación, debe configurar el inicio de sesión en dos pasos que será independiente del correo electrónico de la cuenta de Bitwarden. Esto incluye una aplicación de autenticación, una clave de seguridad o un inicio de sesión en dos pasos basado en correo electrónico con un correo electrónico diferente. Si el usuario tiene activo cualquier método 2FA, se le excluirá de la verificación de nuevo dispositivo basada en correo electrónico. Los usuarios con 2FA activo también deben guardar su código de recuperación de Bitwarden en un lugar seguro.

¿Quién está excluido de esta verificación de nuevos dispositivos basada en el correo electrónico?

Quedan excluidas las siguientes categorías de inicios de sesión:

- Quedan excluidos los usuarios que tengan configurado el inicio de sesión en dos pasos.
- Quedan excluidos los usuarios que inician sesión con SSO, una clave de acceso o con una clave API.
- Quedan excluidos los usuarios autoalojados.
- Quedan excluidos los usuarios que se conecten desde un dispositivo en el que ya se hayan conectado anteriormente.
- Se excluye a los usuarios que se den de baja desde su pantalla **Configuración** → **Mi cuenta** (**No recomendado**).

Mi organización utiliza SSO, ¿tienen mis usuarios que completar la verificación de nuevos dispositivos?

No. Los usuarios que inicien sesión con SSO estarán exentos y no se les pedirá que verifiquen el inicio de sesión en un nuevo dispositivo. Sin embargo, si un usuario, sin el inicio de sesión en dos pasos activado, inicia sesión con un nombre de usuario y una contraseña sin pasar por SSO, se le pedirá que verifique el nuevo dispositivo.

No quiero compartir mi correo electrónico real con Bitwarden, ¿cómo puedo configurar mi cuenta?

Los usuarios que deseen permanecer en el anonimato disponen de varias opciones:

- Utiliza una opción de inicio de sesión en dos pasos que no requiera un correo electrónico, como una aplicación de autenticación, una clave de seguridad o un inicio de sesión en dos pasos basado en correo electrónico con un correo electrónico diferente.
- Utiliza un servicio de reenvío de alias de correo electrónico.
- Bitwarden autoalojado.

Bitwarden anima a los usuarios a tener un correo electrónico activo, ya que Bitwarden envía importantes alertas de seguridad como intentos fallidos de inicio de sesión.

Si utilizo el código de recuperación 2FA en un nuevo dispositivo porque he perdido mi acceso 2FA, ¿seguiré sujeto a esta verificación de nuevo dispositivo?

Bitwarden actualizará el flujo del código de recuperación para que cuando envíe su contraseña y código de recuperación, inicie sesión en la aplicación web y acceda a su configuración 2FA. Si te preocupa la posibilidad de que te bloqueen, deberías **evitar** realizar este proceso en un navegador de incógnito o en un dispositivo con una conectividad a Internet poco fiable para asegurarte de que puedes completar los pasos de configuración necesarios en esta sesión iniciada.

Quiero excluirme. ¿Hay alguna opción?

Se trata de una seguridad añadida para los usuarios que no tienen activado el inicio de sesión en dos pasos. Los usuarios que no tienen activado el inicio de sesión en dos pasos son más vulnerables al acceso no autorizado por parte de atacantes, ya que las contraseñas pueden verse comprometidas de múltiples maneras, incluso si son fuertes y únicas. Por ejemplo, los métodos más habituales son:

- Ataques de phishing: Los ciberdelincuentes utilizan correos electrónicos o sitios web engañosos para que reveles tu contraseña.
- Ingeniería social: Los atacantes pueden intentar manipularle o engañarle para que revele su contraseña a través de llamadas telefónicas, mensajes de texto u otros medios.
- Descifrado de **contraseñas mediante ataques** de fuerza bruta: Los atacantes utilizarán herramientas automatizadas para intentar adivinar repetidamente la contraseña.
- **Keylogging o malware:** Si tu dispositivo está infectado con malware o un keylogger, los atacantes podrían registrar cada pulsación que hagas -incluida tu contraseña- sin tu conocimiento.

Con la verificación de nuevo dispositivo, incluso si su contraseña se ve comprometida a través de uno de los métodos anteriores, el atacante todavía tendría que recuperar la segunda verificación, que es el código de un solo uso en su correo electrónico. Esto reduce significativamente la probabilidad de accesos no autorizados.

La nueva verificación de dispositivos está diseñada para ser menos intrusiva que el inicio de sesión en dos pasos tradicional. Sólo se aplica al iniciar sesión desde un dispositivo o cliente que no se haya utilizado antes, por lo que la mayoría de los usuarios no experimentarán este paso adicional, ya que inician sesión regularmente en sus dispositivos cotidianos. El proceso de verificación utiliza tu correo electrónico, que es algo que mucha gente mantiene abierto en el teléfono o el ordenador, por lo que recuperar el código es rápido y sencillo.

Los usuarios que pueden experimentar algunos problemas son los que hacen lo siguiente:

- No tiene activado el inicio de sesión en dos pasos.
- Almacenar su contraseña de correo electrónico en Bitwarden.
- Desinstalar y reinstalar Bitwarden constantemente.
- Desconectarse de su correo electrónico en todas partes.

Sólo los usuarios que hagan todas estas cosas y cumplan las condiciones anteriores experimentarán problemas con esta actualización de seguridad. Si los usuarios no pueden acceder a su cuenta, pueden ponerse en contacto con Customer Success en Bitwarden.

Si los usuarios no desean la verificación del nuevo dispositivo, se recomienda encarecidamente activar un método alternativo de inicio de sesión en dos pasos (ya sea mediante una aplicación de autenticación, una llave de hardware o un correo diferente) para proteger su cuenta.

Si los usuarios no desean la verificación de nuevos dispositivos, no quieren configurar un método alternativo de inicio de sesión en dos pasos y **no quieren ningún tipo de seguridad en su cuenta,** existe la opción de excluirse navegando hasta la pantalla **Configuración → Mi cuenta** y desplazándose hasta la sección Zona peligrosa. Debemos hacer hincapié en que esto no es **muy recomendable**, ya que deja su cuenta vulnerable a diversos ataques.