bitwarden | Hilfezentrum Artikel

New Device Login Protection (February / March 2025)

Ansicht im Hilfezentrum:
https://bitwarden.com/de-de/help/new-device-verification/#print

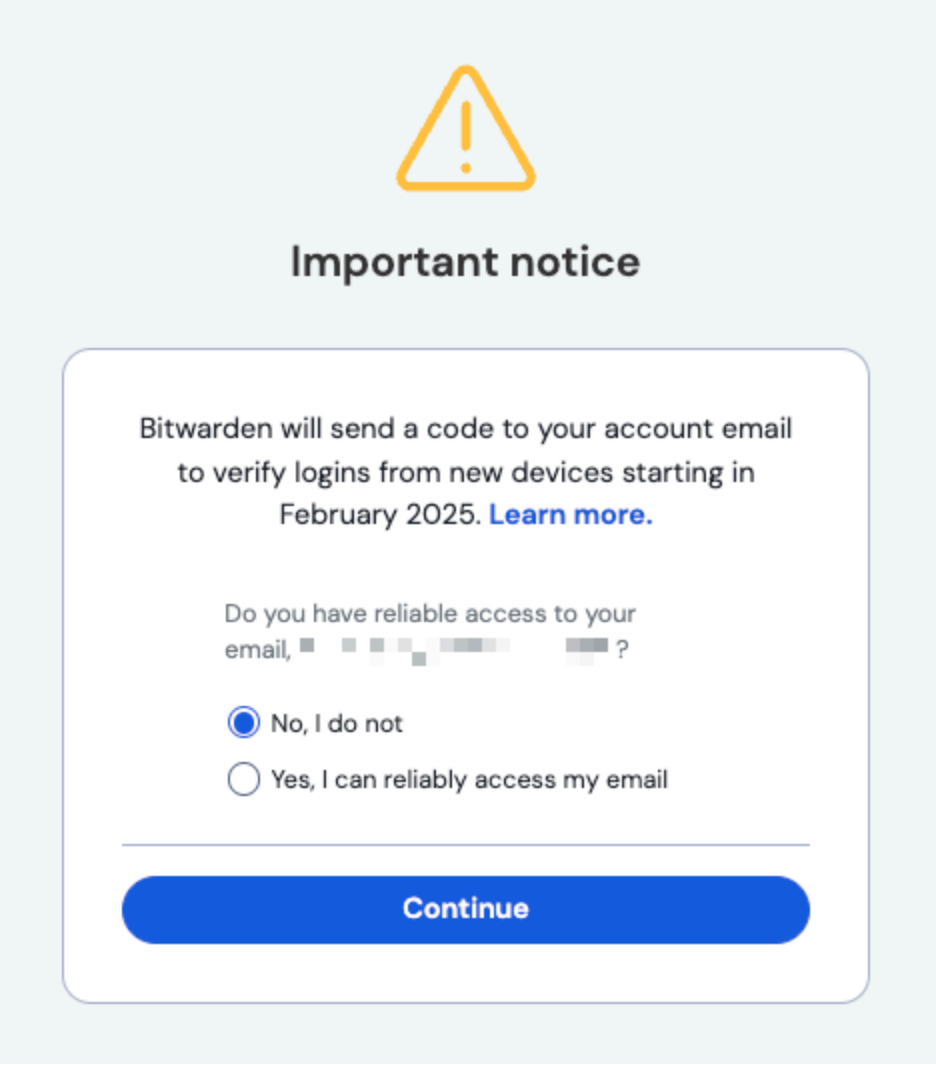
New Device Login Protection (February / March 2025)

To keep your account safe and secure, starting sometime February / March 2025, Bitwarden will require additional verification **for users who do not use two-step login**. After entering your Bitwarden master password, you will be prompted to enter a one-time verification code sent to your account email to complete the login process **when logging in from a device you have not logged in to previously**. For example, if you are logging in to a mobile app or a browser extension that you have used before, you will not receive this prompt.

Most users will not experience this prompt unless they are frequently logging into new devices. This verification is only needed for new devices or after clearing browser cookies.

If you regularly access your email, retrieving the verification code should be straightforward. If you prefer not to rely on your Bitwarden account email for verification, you can set up two-step login through an Authenticator app, a hardware key, or two-step login via a different email.

Users affected by this change will see the following in-product communication and should have received an email informing them of the change:



New device verification announcement

FAQs

When will this happen?

This change will go into effect starting sometime February / March 2025. This page will be updated once a date has been defined for the release.

Why is Bitwarden implementing this?

Bitwarden is implementing this change to enhance security for users who don't have two-step login activated. If someone gains access to your password, they still won't be able to log into your account without secondary verification (the code sent to your email). This extra layer helps protect your data from hackers who often target weak or exposed passwords to gain unauthorized access.

When will I get prompted for this verification?

You will only get prompted for this verification when logging in from new devices. If you're logging into a device that you've used before, you will not be prompted.

What is considered a new device?

A new device is any device that hasn't been previously used to log into your Bitwarden account. This could include a new phone, tablet, computer, or browser extension that you've never logged in from before. When you log in from a new device, you'll be asked to verify your identity via a one-time code sent to your email.

Other scenarios that will initiate a new device will be:

- Uninstalling and reinstalling the mobile, desktop app, or browser extension will initiate a new device.
- Clearing browser cookies will initiate a new device for the web app, but not for browser extensions.

My email credentials are saved in Bitwarden. Will I be locked out of Bitwarden?

Email verification codes will only be required on new devices for users that do not have two-step login enabled. You will not see this prompt on previously logged in devices and you will log in as normal with your account email and your master password.

If you are logging into a new device, your Bitwarden account email will receive a one-time verification code. If you have access to your email, i.e. a persistent logged in email on your mobile phone, then you will be able to grab the one-time verification code to log in. Once logged in to the new device, you will not be prompted again for the verification code.

If you regularly log into your email using credentials saved in Bitwarden or do not want to rely on your email for verification, you should set up two-step login that will be independent from the Bitwarden account email. This includes an authenticator app, security key, or email-based two-step login with a different email. Having any 2FA method active will opt the user out of the email-based new device verification. Users with 2FA active should also save their Bitwarden recovery code in a safe place.

Who is excluded from this account email-based new device verification?

The following categories of logins are excluded:

- Users who have two-step login set up are excluded.
- Users who log in with SSO, a passkey, or with an API key are excluded.
- Self-hosted users are excluded.
- Users who log in from a device where they have previously logged in are excluded.
- Users who opt-out from their account settings, to which an option will be added, are excluded (**Not recommended**).

My organization uses SSO, do my users have to complete new device verification?

No. Users logging in with SSO will be exempt and not asked to verify the login on a new device. However, if a user, without two-step login enabled, logs in with a username and password without going through SSO, they will be asked to verify the new device.

I do not want to share my real email with Bitwarden, how can I set up my account?

Users who want to remain anonymous have several options available:

- Use a two-step login option that doesn't require an email, including an authenticator app, security key, or email-based two-step login with a different email.
- Use an email alias forwarding service.
- Self-host Bitwarden.

Bitwarden encourages users to have an active email, as Bitwarden sends important security alerts like failed login attempts.

If I use the 2FA recovery code on a new device because I've lost my 2FA access, will I still be subject to this new device verification?

Bitwarden will be updating the recovery code flow so that when you submit your password and recovery code, you are logged into the web app and taken to your 2FA settings. If you are concerned about being locked out, you should **avoid** going through this flow in an incognito browser or on a device with unreliable internet connectivity to make sure you can complete any necessary setup steps in this logged in session.

I want to opt-out! Is there an option to?

This is added security for users that do not have two-step login enabled. Users that do not have two-step login enabled are more vulnerable to unauthorized access by attackers because passwords can be compromised in multiple ways, even if they are strong and unique. For example, common methods include:

- **Phishing attacks:** Cybercriminals use deceptive emails or websites to trick you into revealing your password.
- **Social engineering**: Attackers may attempt to manipulate or deceive you into revealing your password through phone calls, texts, or other means.
- **Password cracking via brute-force attack**s: Attackers will use automated tools to repeatedly try guesses for the password.
- **Keylogging or malware:** If your device is infected with malware or a keylogger, attackers could record every keystroke you make—including your password—without your knowledge.

With new device verification, even if your password is compromised through one of the methods above, the attacker would still need to retrieve the second verification, which is the one-time code in your email. This significantly reduces the likelihood of unauthorized access.

New device verification is designed to be less intrusive than traditional two-step login. It only applies when logging in from a device or client you haven't used before, so most users won't experience this extra step, as they're regularly logging in on their everyday devices. The verification process uses your email, which is something many people keep open on a phone or computer, so retrieving the code is quick and easy.

Users that may experience some challenges are those do the following:

- Do not have two-step login enabled.

- Store their email password in Bitwarden.
- Constantly uninstall and reinstall Bitwarden.
- Log out of their email everywhere.

Only users that do all these things and match the conditions above will experience friction with this security update. If users do get locked out of their account, they can reach out to Customer Success at Bitwarden.

If users do not want new device verification, it is strongly recommended to turn on an alternate two-step login method (either via an authenticator app, hardware key, or a different mail) to protect your account.

If users do not want new device verification, do not want to set up an alternate two-step login method, and **do not want any security on their account,** there will be an option to turn off new device verification in the Danger Zone settings when the feature goes live. However, we must emphasize that this is **strongly not recommended**, as it leaves your account vulnerable to various attacks.