

# Secure Account Access

## Securing Access

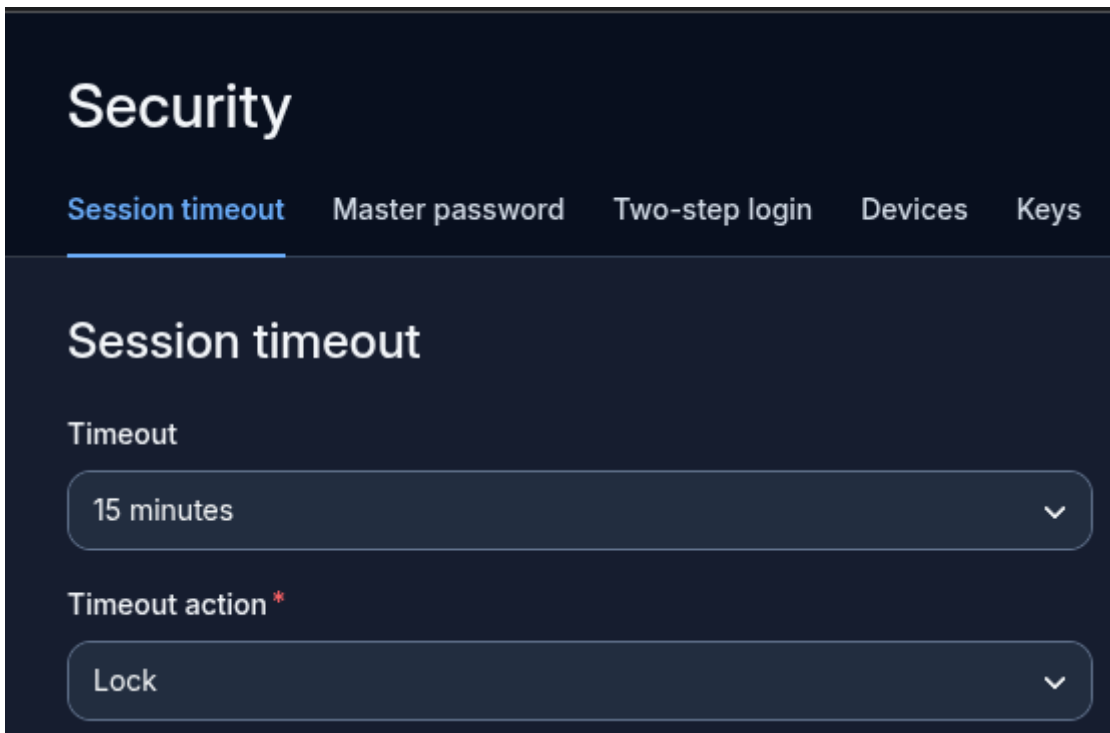
Once logged in, Bitwarden uses insecure settings by default. It is strongly recommended to do the following steps

### Session Timeouts

Setting session timeouts is essential to prevent anyone with physical access to your devices from stealing passwords

### Web Vault

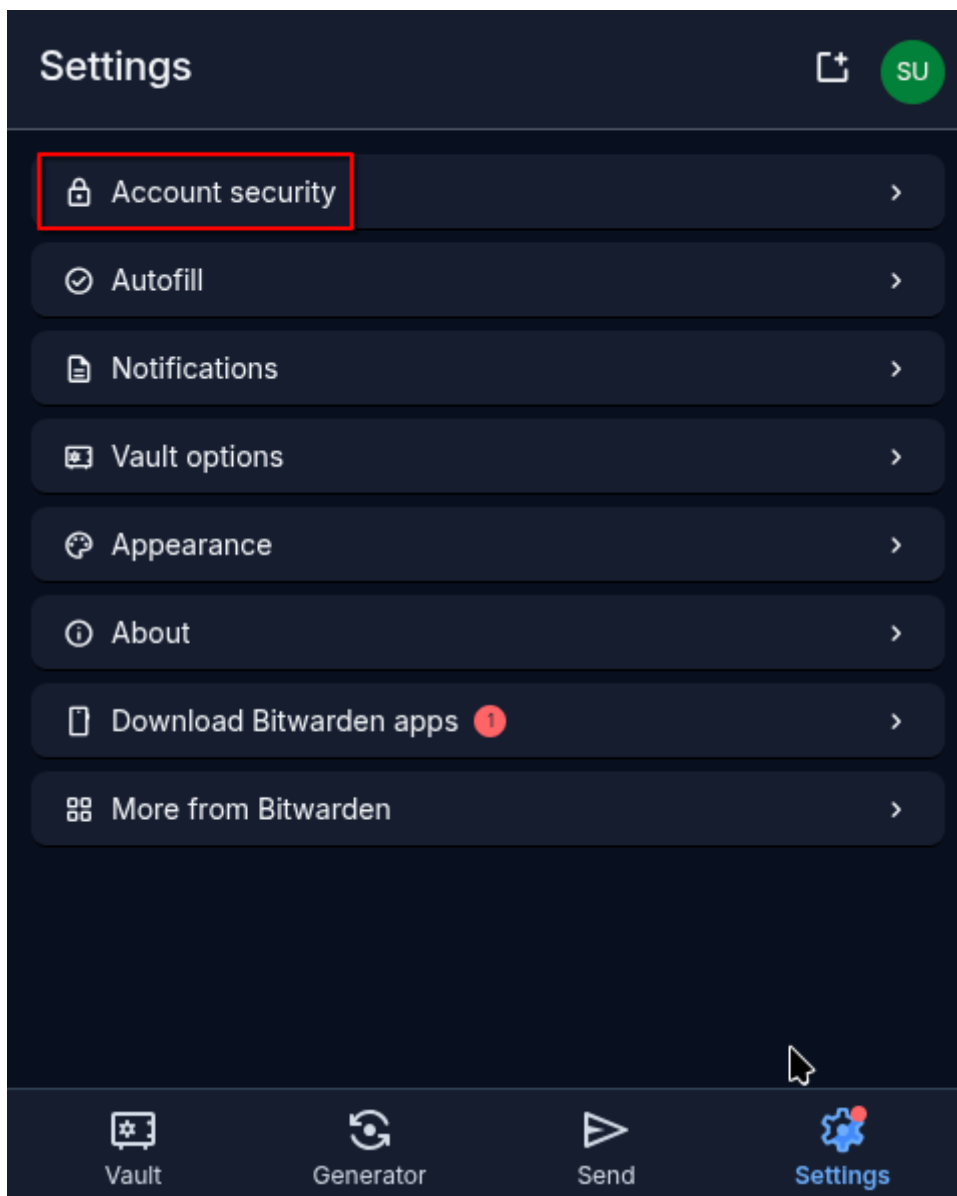
Once logged in, go to Settings -> Security -> Session timeout. Set the timeout to something you're comfortable with.



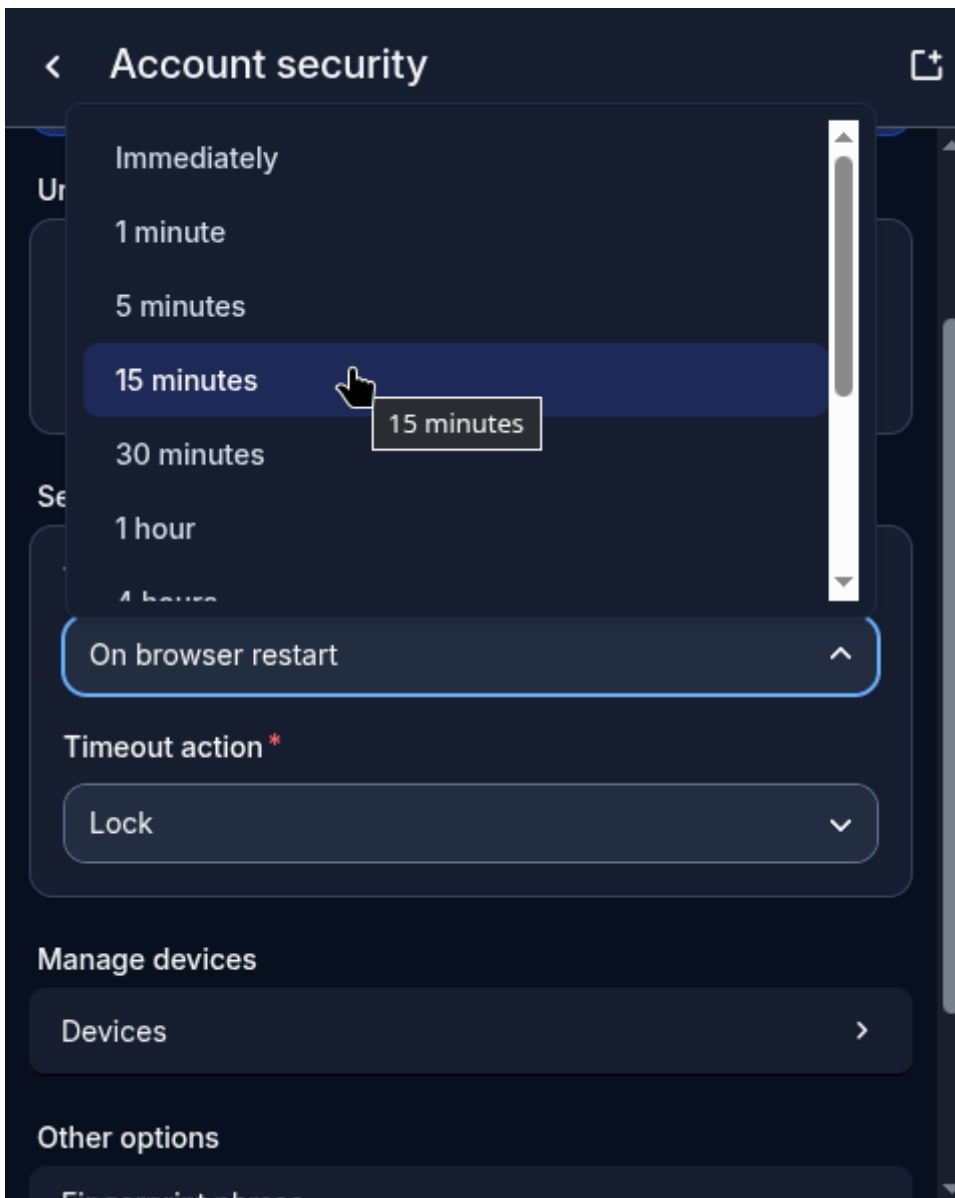
The screenshot shows the Bitwarden web interface. At the top, the word "Security" is displayed in a large, white font. Below it, there are five tabs: "Session timeout" (which is highlighted with a blue underline), "Master password", "Two-step login", "Devices", and "Keys". The "Session timeout" section is active, showing two settings: "Timeout" set to "15 minutes" and "Timeout action" set to "Lock". Both settings are displayed in a dark blue rounded rectangle with a white dropdown arrow on the right.

### Browser Extension

Once logged in, got to Settings -> Account security



Set the Session timeout to something you're comfortable with.



## Mobile App

This process is very similar to "Browser Extension". Find Account security and set the Session timeout

## Two-factor Login (TFA)

Your passwords protect you, your vault protects your passwords. Protect your vault.

This step must be performed in the Web Vault at <https://warden.firehawk-systems.com>

Once logged in, navigate to Settings -> Security -> Two-step login



Vaults

Send

Tools

Reports

Settings

My account

Security

Appearance

Domain rules

Emergency access

Security

Session timeoutMaster passwordTwo-step loginDevicesKeys

Two-step login

Secure your account by requiring an additional step when logging in.

Warning

Your single-use recovery code can be used to turn off two-step login in the event that you lose access to your two-step login provider. Bitwarden recommends you write down the recovery code and keep it in a safe place.

View recovery code

Providers

Email

Enter a code sent to your email.

Manage

Authenticator app

Enter a code generated by an authenticator app like Bitwarden Authenticator.

Manage

Passkey

Use your device's biometrics or a FIDO2 compatible security key.

Manage

Duo

Enter a code generated by Duo Security.

Manage

If you have a YubiKey and know how to use it, select Passkey. Otherwise select the "Manage" button next to Email. You will be prompted for your password again.

Do not select Authenticator app unless you know what you are doing, Bitwarden app should never be used for this

Two-step login Email

×

Follow these steps to set up two-step login with email:

1. Enter the email that you wish to receive verification codes \*

Send email

2. Enter the resulting 6 digit verification code from the email \*

123456

Turn onClose

Enter the code that gets sent once 'Send email' is clicked. A green tick will appear next to Email when successful

## Save Recovery Code

The recovery code is required to regain access to your account if the primary TFA method fails, and should be stored somewhere safe.

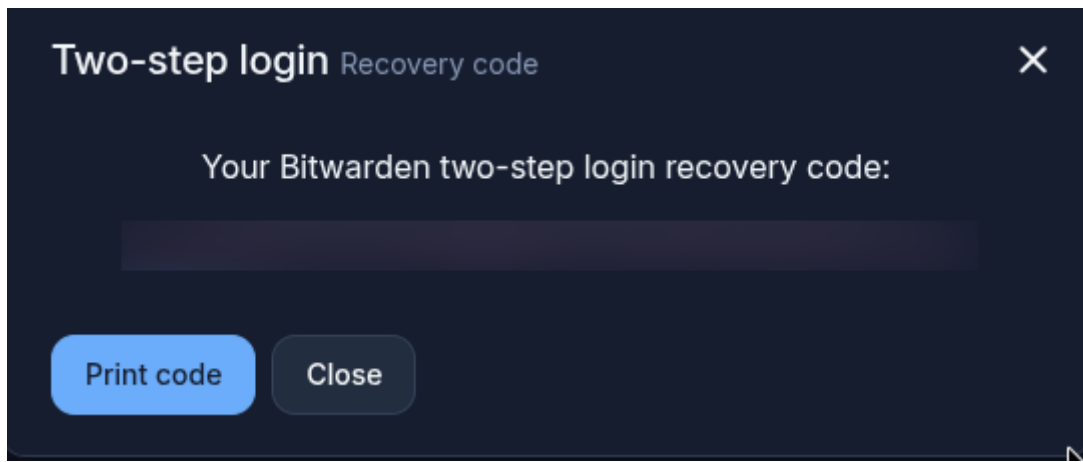
In the warning box, click "View recovery code". You will be prompted for your password again.

ⓘ Warning

Your single-use recovery code can be used to turn off two-step login in the event that you lose access to your two-step login provider. Bitwarden recommends you write down the recovery code and keep it in a safe place.

View recovery code

Highlight and copy the pink text, then save somewhere safe.



## You have completed the securing of your Bitwarden Account

---

Revision #2

Created 2026-09-12 08:20:25 UTC by The Firehawk

Updated 2026-09-12 08:32:19 UTC by The Firehawk