



NOW MORE THAN EVER YOUR TRUSTED MANAGED I.T. SERVICES PARTNER

Bitwarden Quick Guide

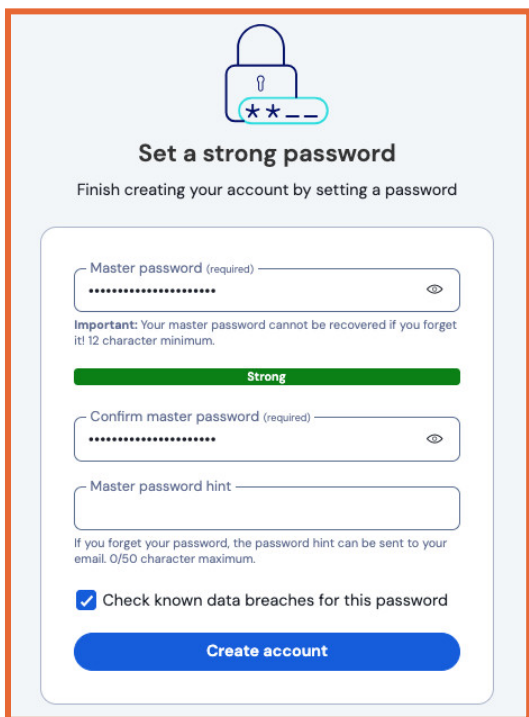
 **bitwarden**

A quick, easy-to-read guide for using Bitwarden, so you can manage and share passwords safely and confidently.

1. Getting Started

Join Your Organization

- Look for an invitation in your work email. Accept it. If you don't already have a Bitwarden account, you'll be prompted to create one.
- If your company uses Single Sign-On (SSO), logging in via that may automatically join you.



The screenshot shows the 'Set a strong password' step of the Bitwarden account creation process. It includes fields for a master password, a confirmation, and a hint, along with a strength indicator and a checkbox for checking data breaches.

Set a strong password
Finish creating your account by setting a password

Master password (required) [password field] [eye icon]

Important: Your master password cannot be recovered if you forget it! 12 character minimum.

Strong

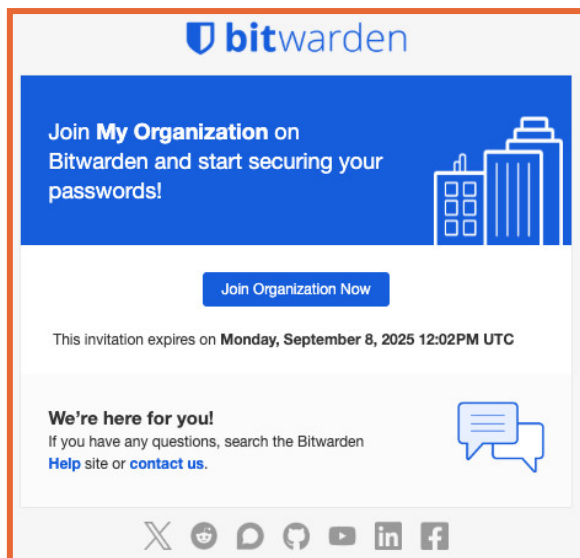
Confirm master password (required) [password field] [eye icon]

Master password hint [text field]

If you forget your password, the password hint can be sent to your email. 0/50 character maximum.

☒ Check known data breaches for this password

Create account

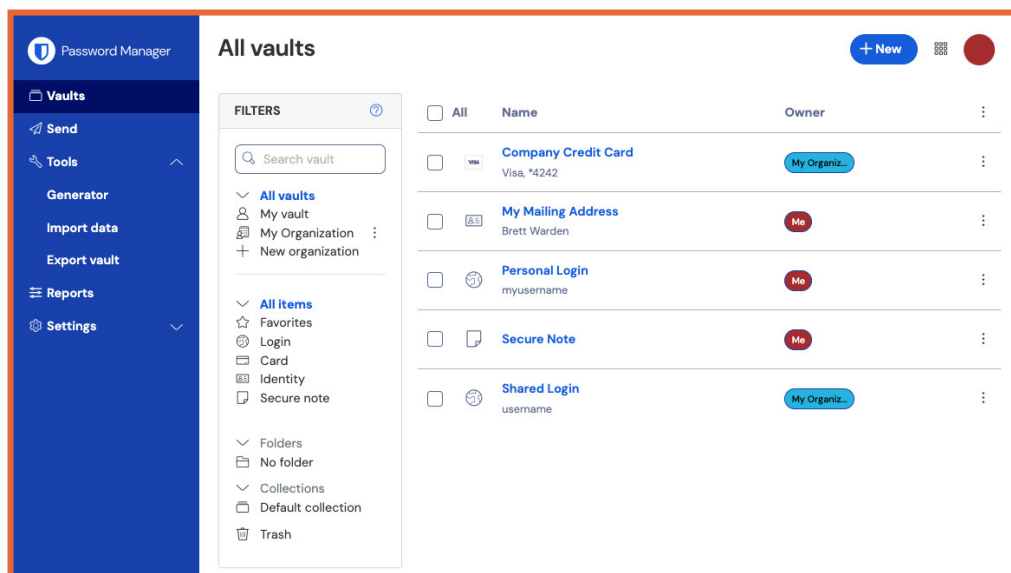


Choose Your Master Password

- You'll either set a master password or log in using a trusted device, depending on your company's setup.
- Master password must be **memorable** (the company cannot retrieve it for you) and **strong** (min 14 characters long, uncommon).

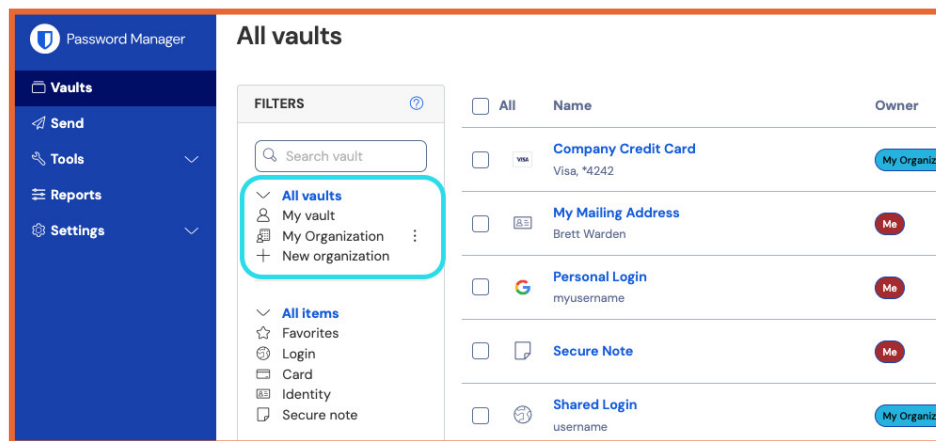
2. Your Vault and What It Does

- Your vault is your secure space to store logins, cards, identities, and secure notes.
- Everything you save syncs across your devices, so you can access passwords anywhere.
- You can import passwords from your browser or another manager to save time.



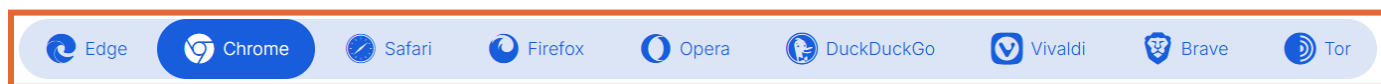
3. Shared Access (Team Use)

- **Shared vault:** As an organization member, securely access and share team logins and company cards via the shared vault.
- Shared items are organized into **Collections** which are grouped by category, such as:
 - Business unit: e.g., “Sales Team”
 - Business function: e.g., “Social Media Logins”
 - System: e.g., “AWS Credentials”

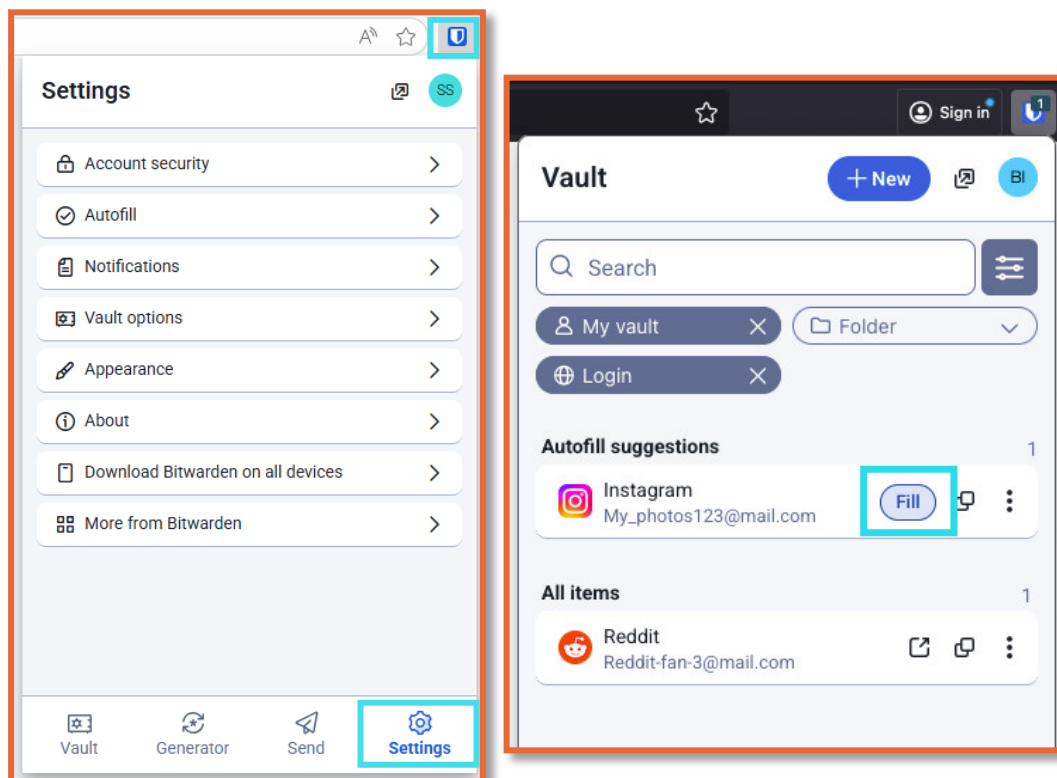


4. Use Bitwarden While Browsing

- [Download](#) and install the Bitwarden browser extension into your favorite web browser



- Set up Autofill: Within the browser extension, go to **Settings** → **Autofill** to turn on autofill.
- Fill logins: On a website login page, click the Bitwarden icon and select the matching credential to autofill username and password.



5. Enable Multi-Factor Authentication

- MFA adds a critical second layer of security on top of your master password.
- Even if someone steals your password, they cannot access your vault without the second factor.
- Strongly recommended for all users to maximize protection of personal and team passwords.

Good Habits:

- Master password: Keep it unique and never reuse.
- Stay organized: Save new passwords immediately.
- Autofill: Reduces errors and weak passwords.
- Shared items: Add to collections only if needed by the team.
- Need help: Contact IT for login or access issues.

If you have any questions about NetExtender, please feel free to contact your IT professionals at:

support@cleverdogit.com.

Or, if there's anything else you need us to work on, you can email help@cleverdogit.com to create a new ticket.