

DOCS > PASSWORD MANAGER > YOUR VAULT > VAULT ITEMS

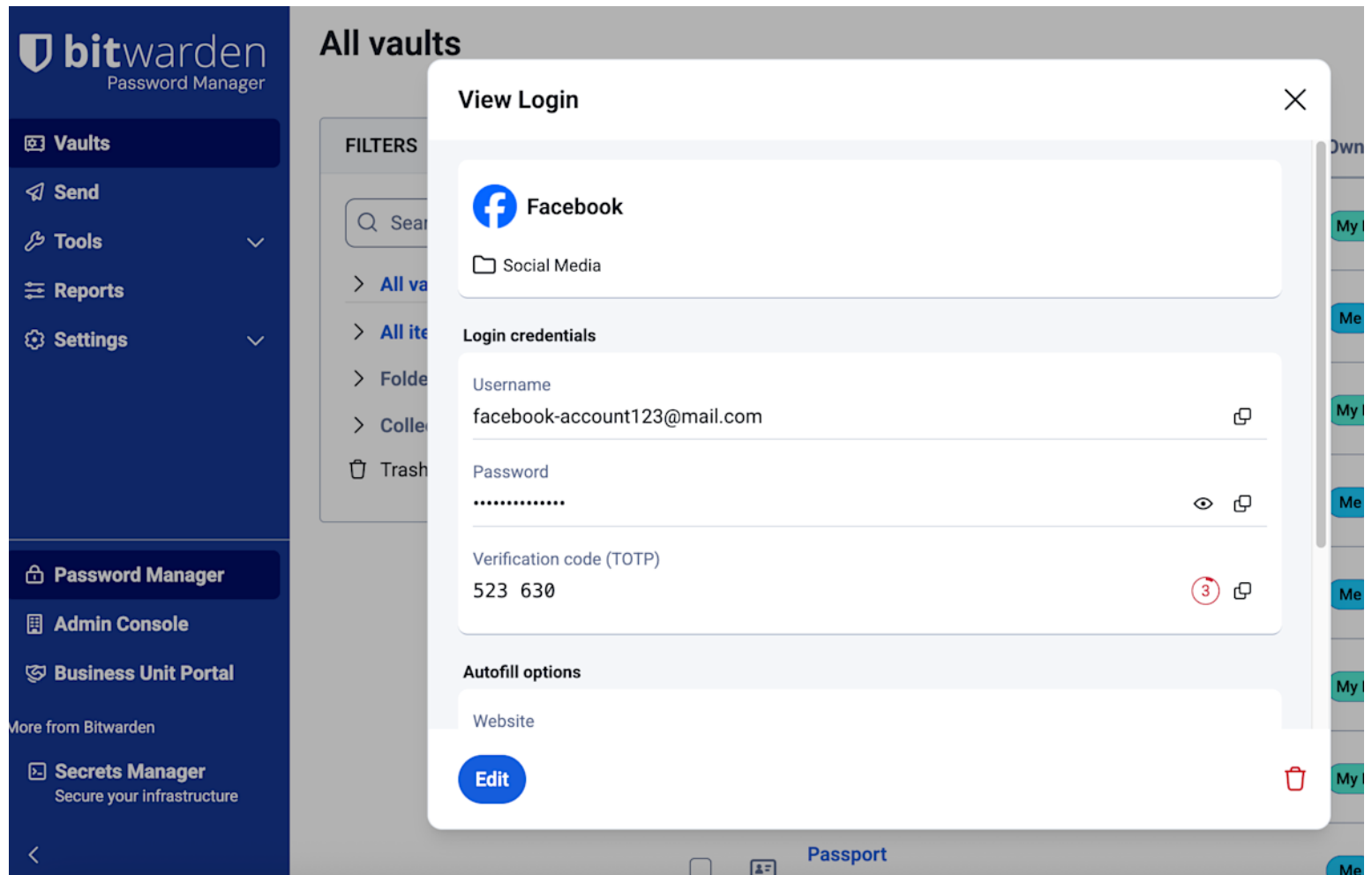
Item Types

Item Types

Did you know that Bitwarden can securely store more than just usernames and passwords? There are five types of items you can store in your vault; logins, cards, identities, secure notes, and SSH keys:

⇒Logins

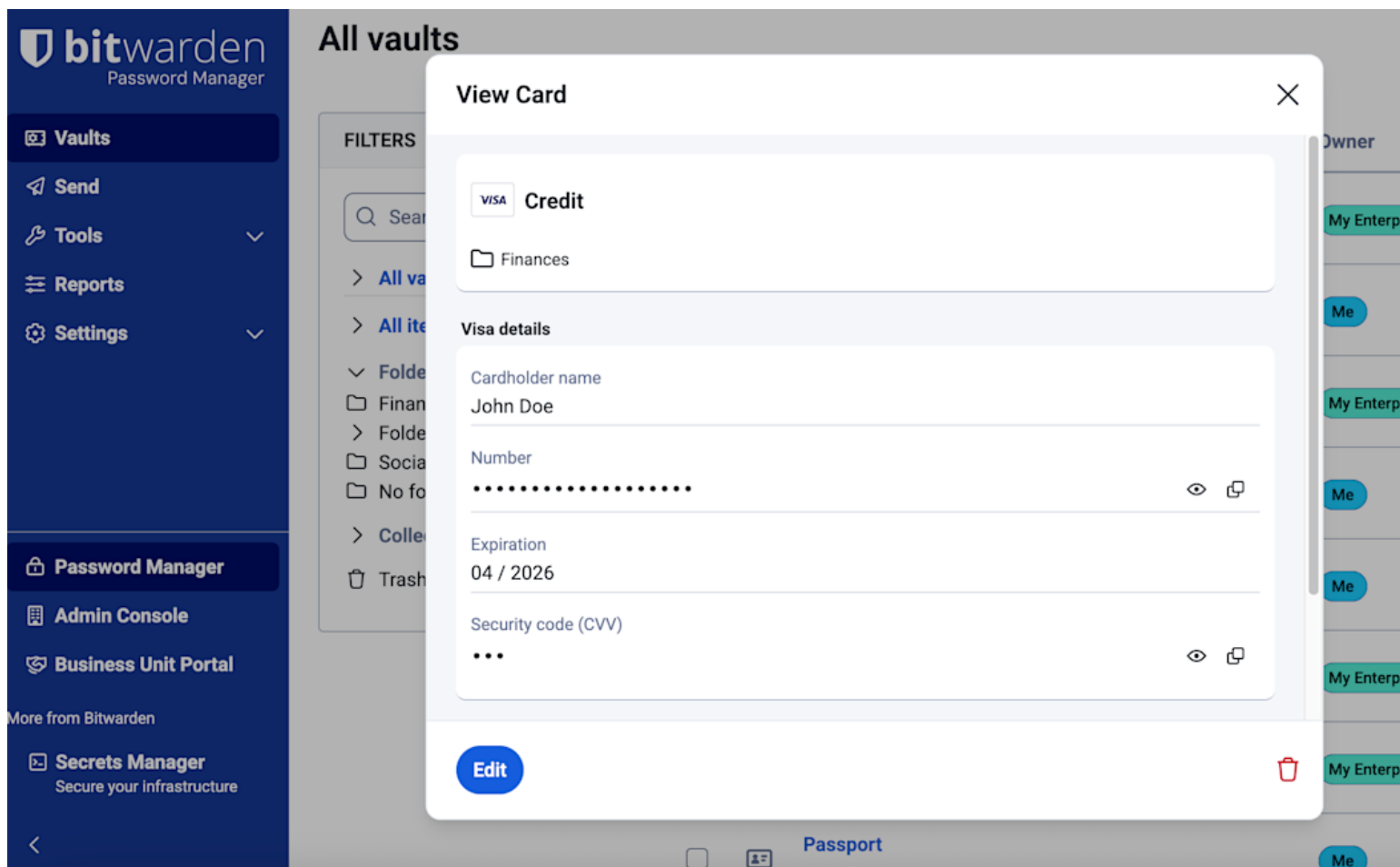
Logins are most often used to store username and password combinations, passkeys, and support [TOTP seeds](#) for premium users. Whatever plan you are on, we recommend giving every login a [URI for easy autofill](#):



Login item

⇒Cards

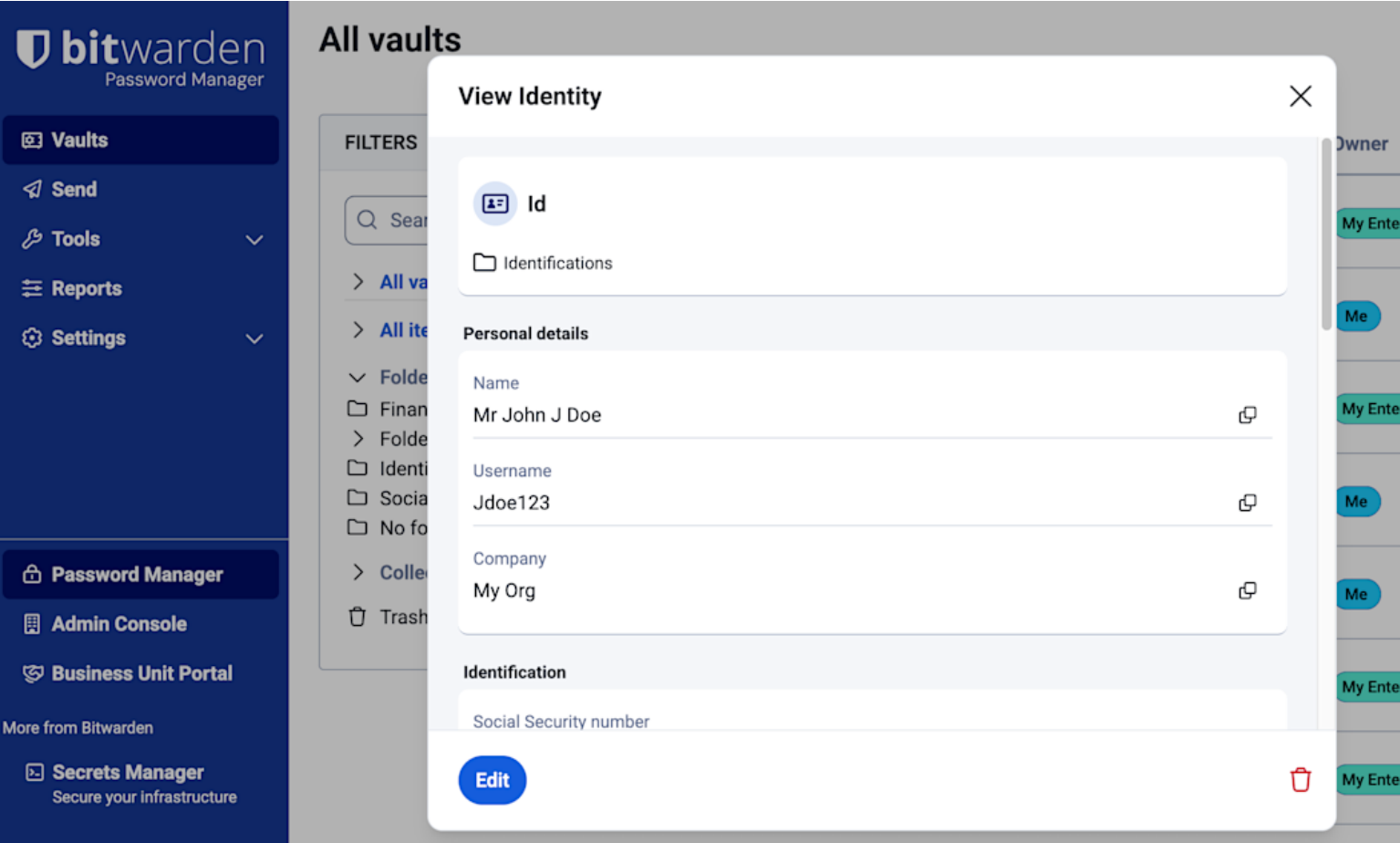
Cards can be used to securely store credit or debit card information:



Card item

⇒Identities

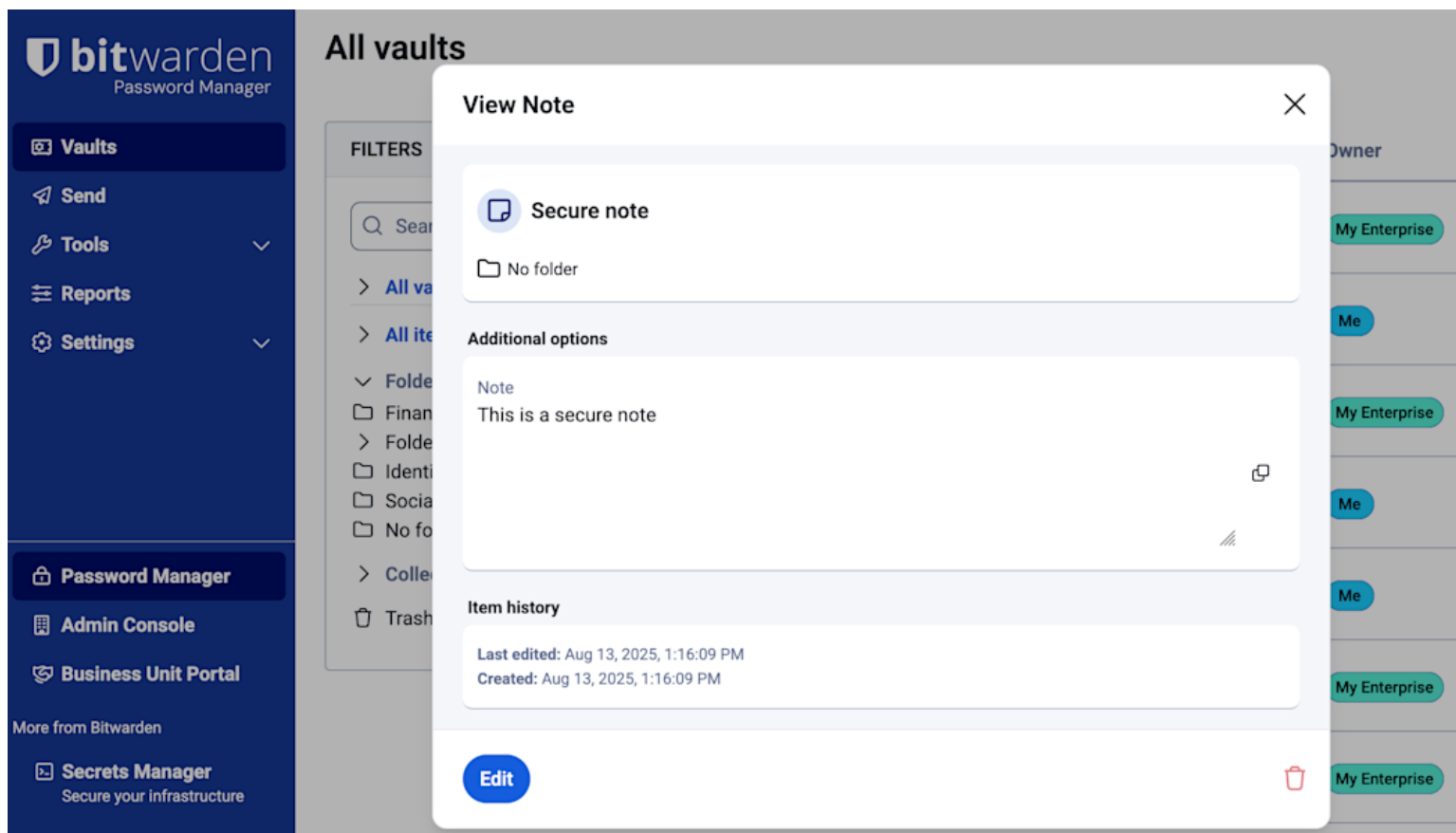
Identities can be used to store billing, mailing, and most other types of information you might need when filling out online forms:



Identity item

⇒Secure notes

Secure notes can be used to store encrypted freeform text for anything you want protected:



Secure note item



Tip

You can [import items](#) directly into your vault from most password managers or web browsers.

Individual & organizational vaults

Many Bitwarden users will have access to an individual vault and an organization vault. Learn how to use and manage each vault effectively:

Individual and Organization vaults

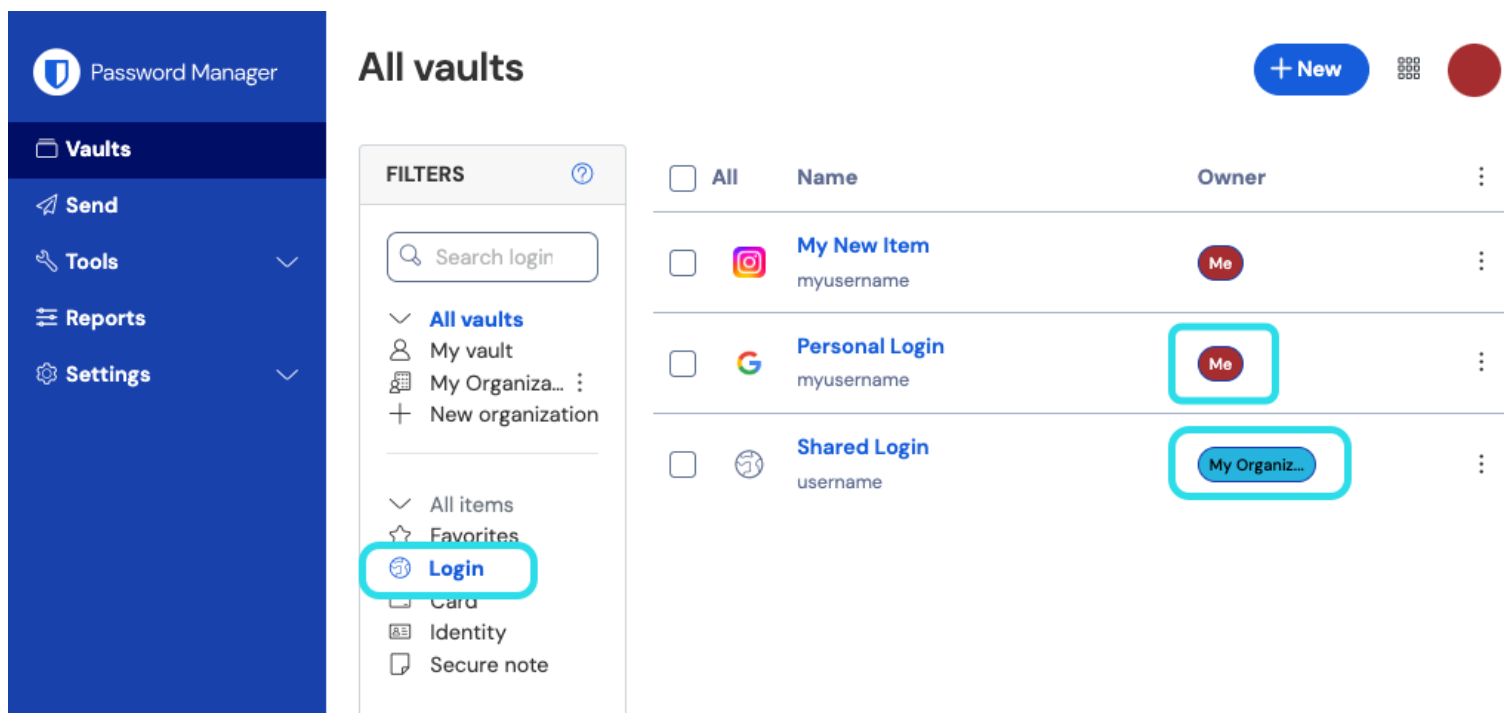
Filter vault items

You can filter which items to list by a few different characteristics. To filter vault items:

⇒Web app

Either:

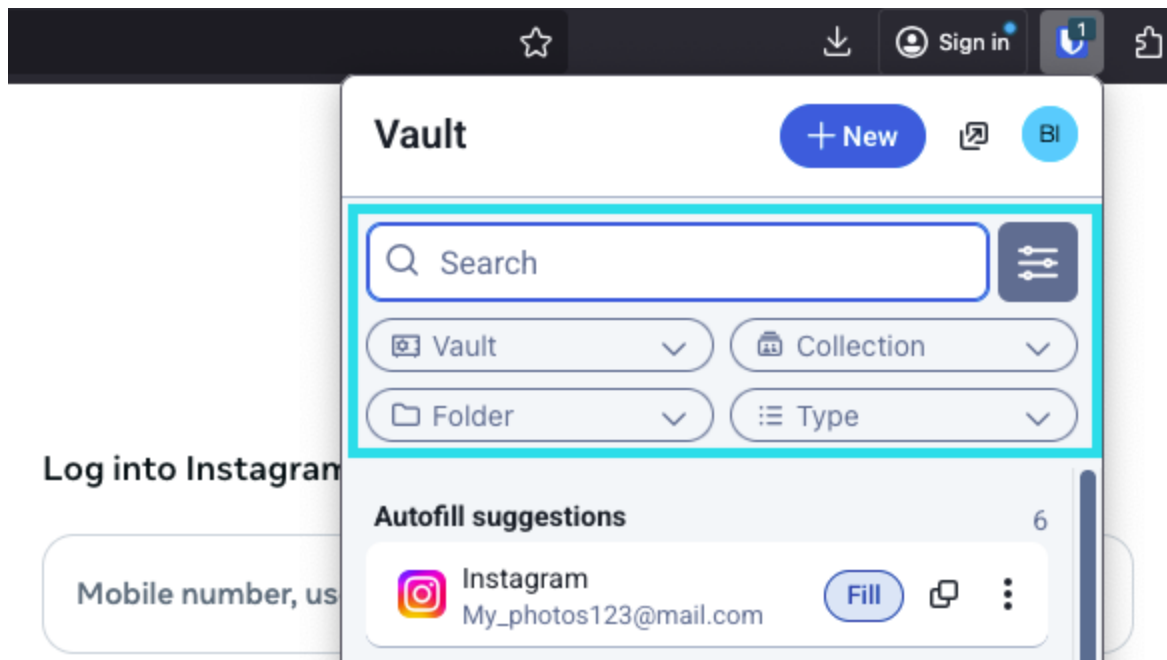
- Select a characteristic from the **Filter** column (in the following screenshot, **Login**).
- Select one of the colored cards next to an item (in the following screenshot, either **Me** or **My Organization**).



Web app filtering

⇒Browser extension

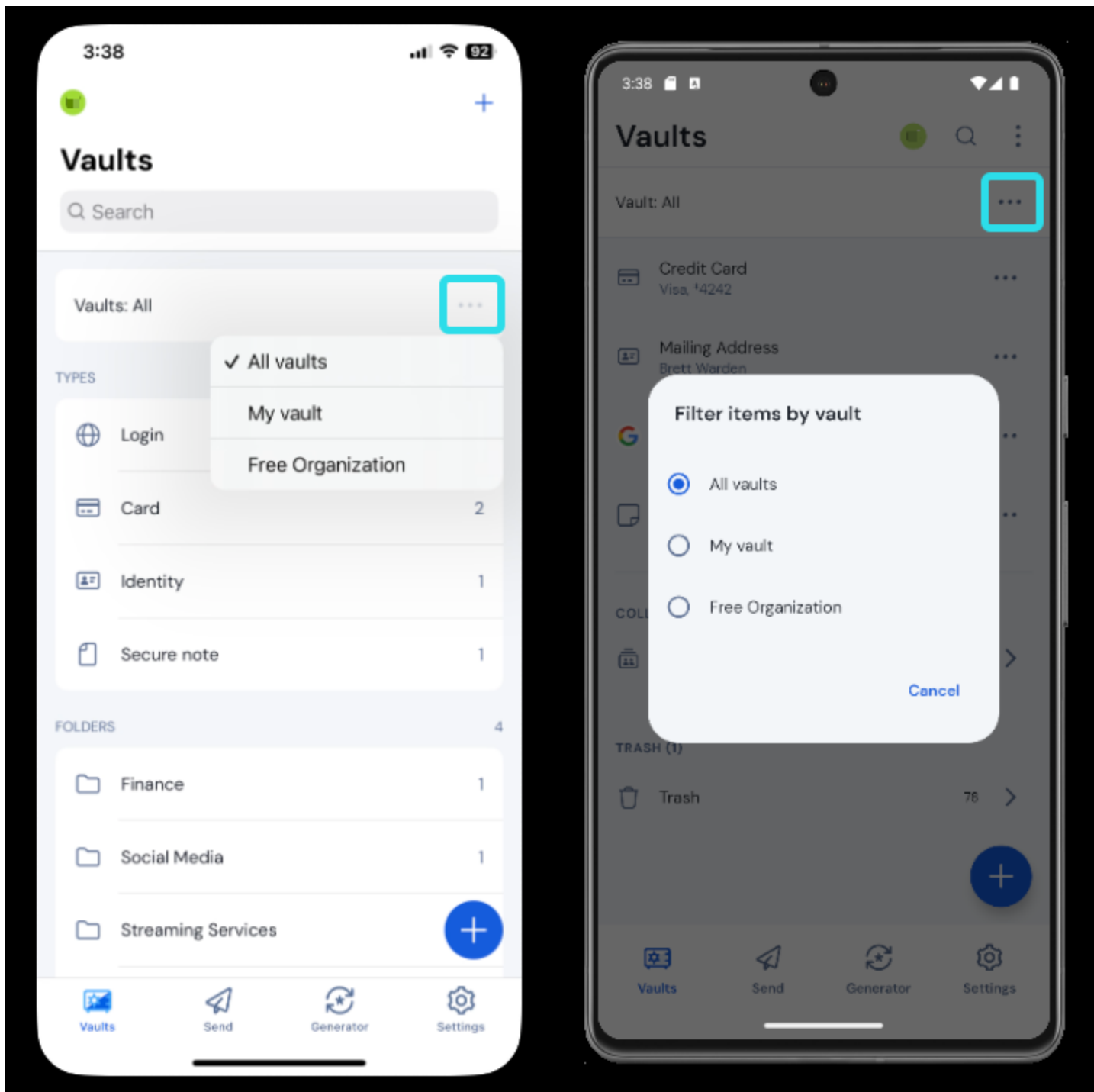
Use the **Vault**, **Collection**, **Folder**, or **Type** selectors at the top of the **Vault** tab. You can turn show and hide the filter dropdown menus with the button:



Browser extension filters and suggestions

⇒Mobile

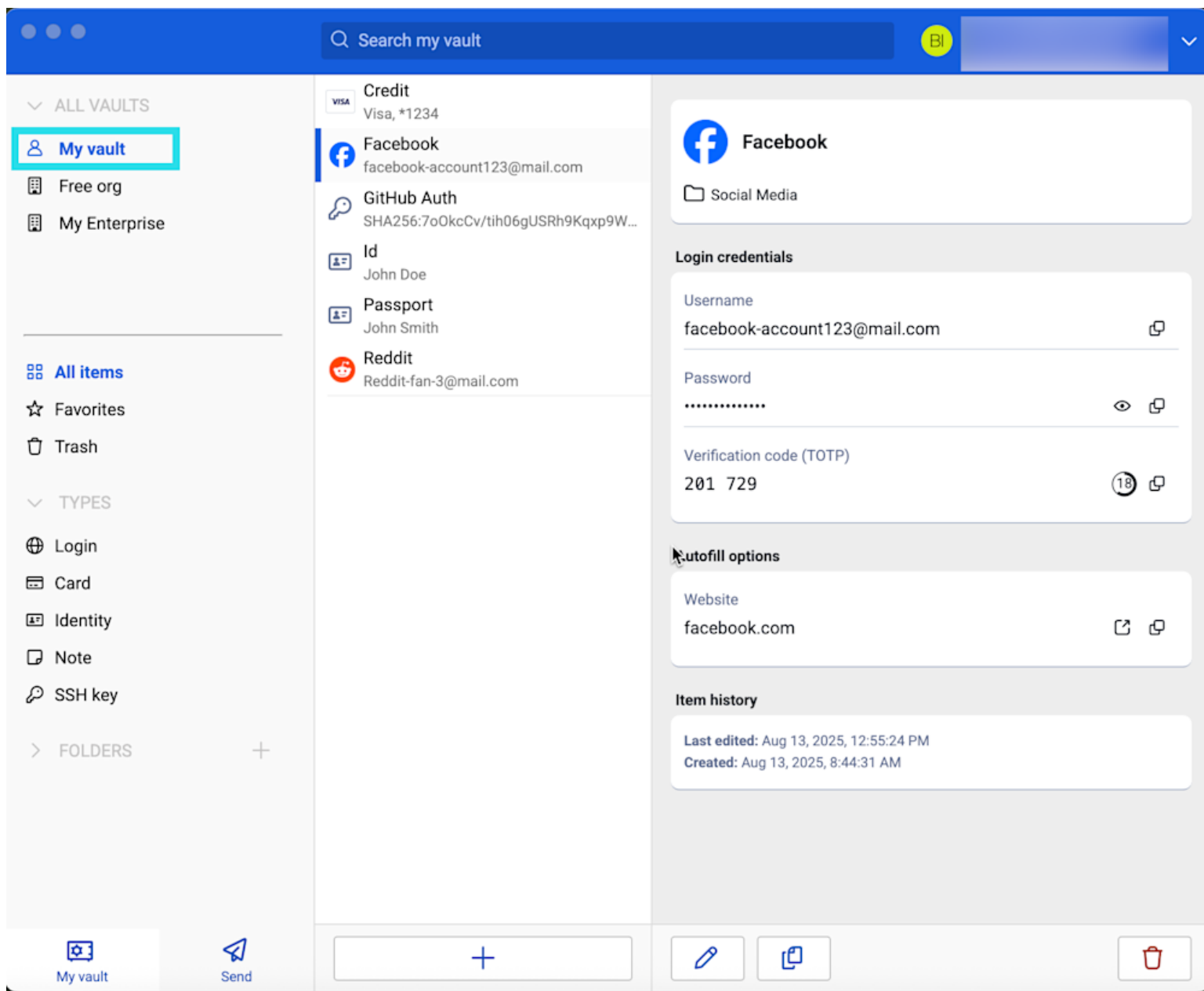
Choose a vault by selecting the **Vault** menu button () on the **Vaults** tab:



Filter vaults on mobile

⇒Desktop

Select a vault from the left-most column (in the following screenshot, **My Vault** or **My Organization**):



Desktop Filtering

⇒CLI

Use the `bw list` command with the `--organizationid` option, which can take either an organization identifier or `null`, to list items by vault. [Learn more](#).

Manage vault items

You can add, edit, and [delete](#) vault items from any Bitwarden app:

⇒Web app

Password Manager

Vaults

Send

Tools

Reports

Settings

Filters

Search vault

All vaults

My vault

My Organiza...

New organization

All items

Favorites

Login

Card

Identity

Secure note

Folders

Important It...

No folder

All

Name

Owner

Company Credit Card

Visa, *4242

My Organiz...

My Mailing Address

Brett Warden

Me

My New Item

myusername

M

Personal Login

myusername

M

Secure Note

Me

Shared Login

username

Attachments

Clone

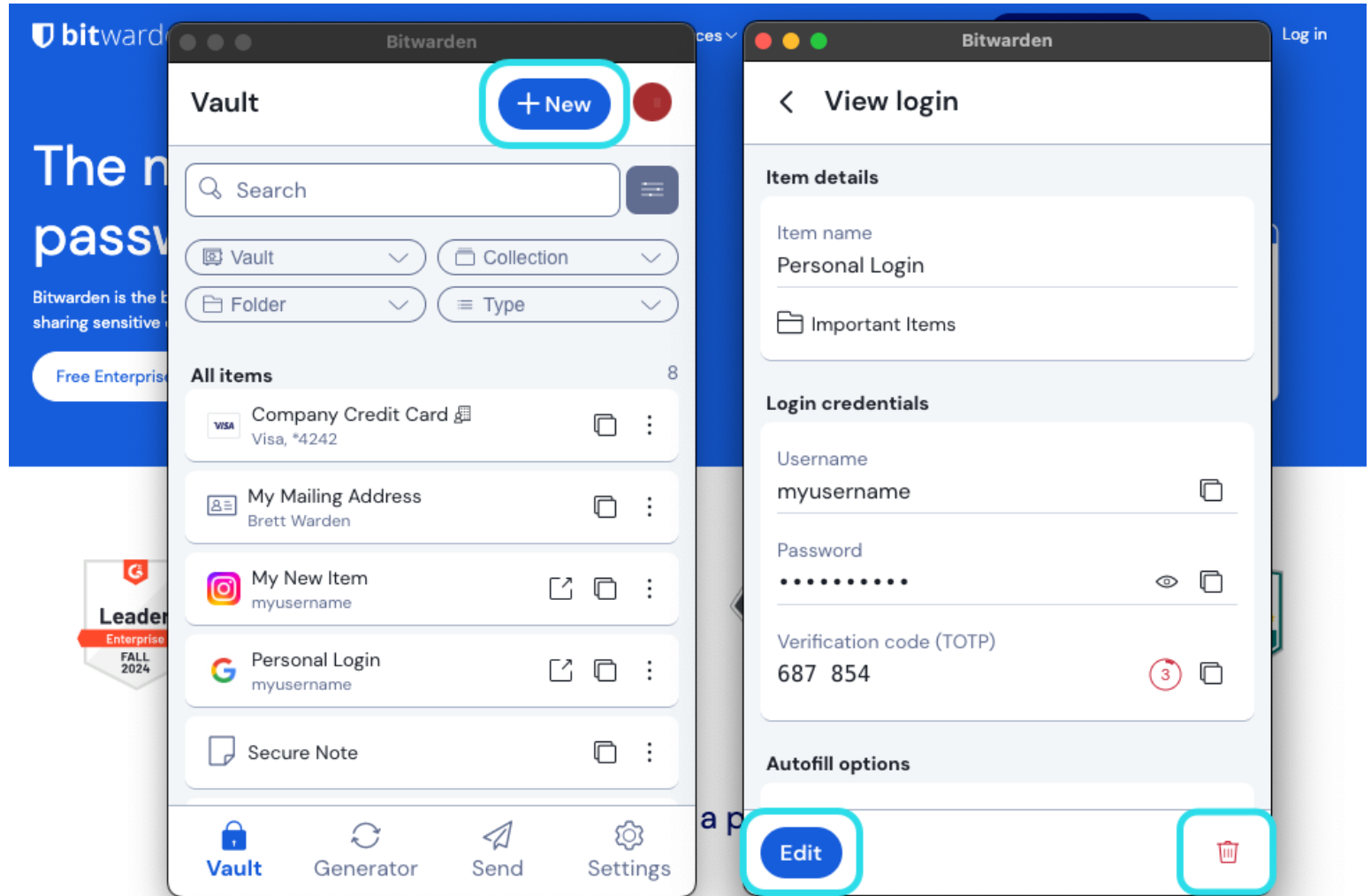
Assign to collections

Delete

Once you open an item, select Edit.

Manage an Item

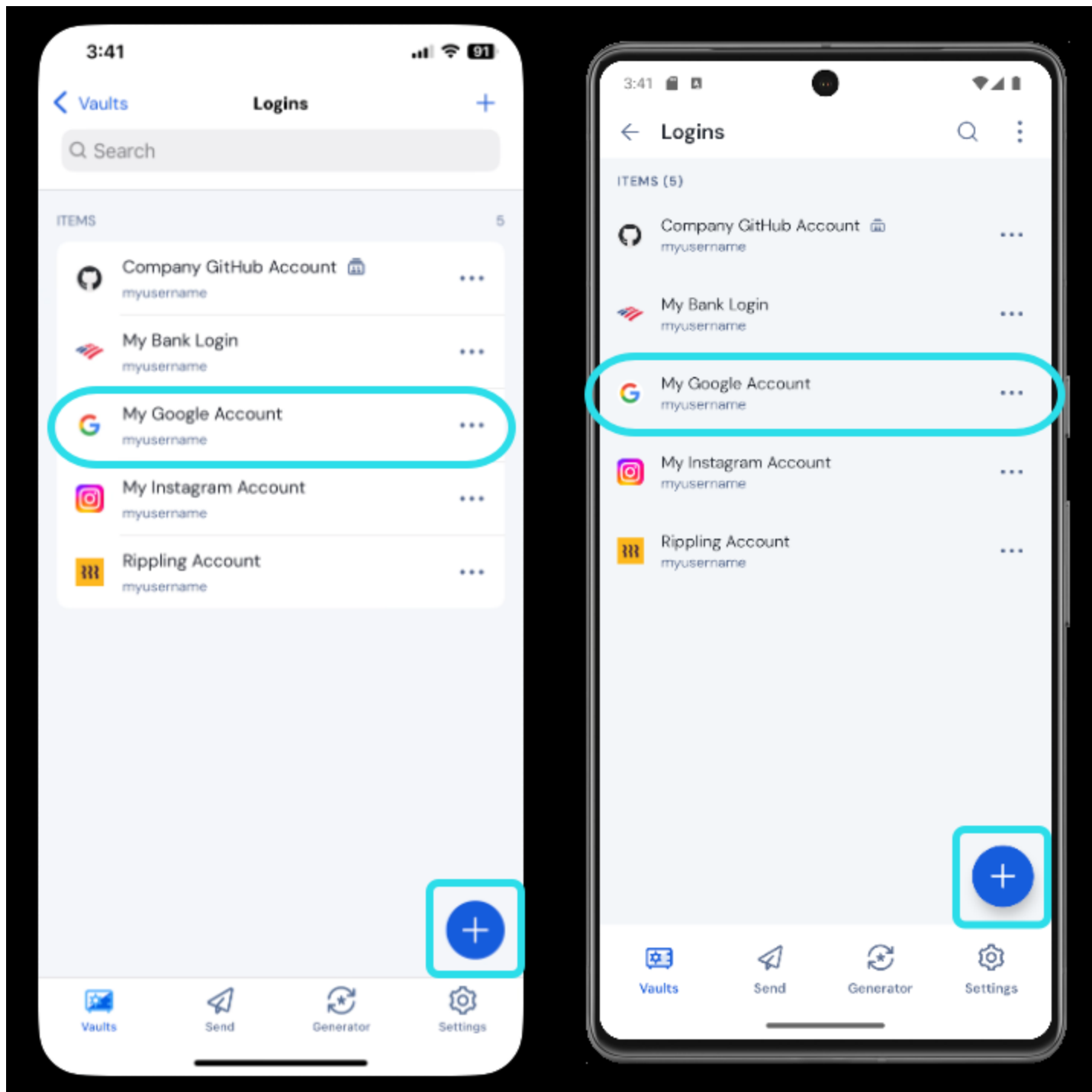
⇒Browser extensions



Manage an item

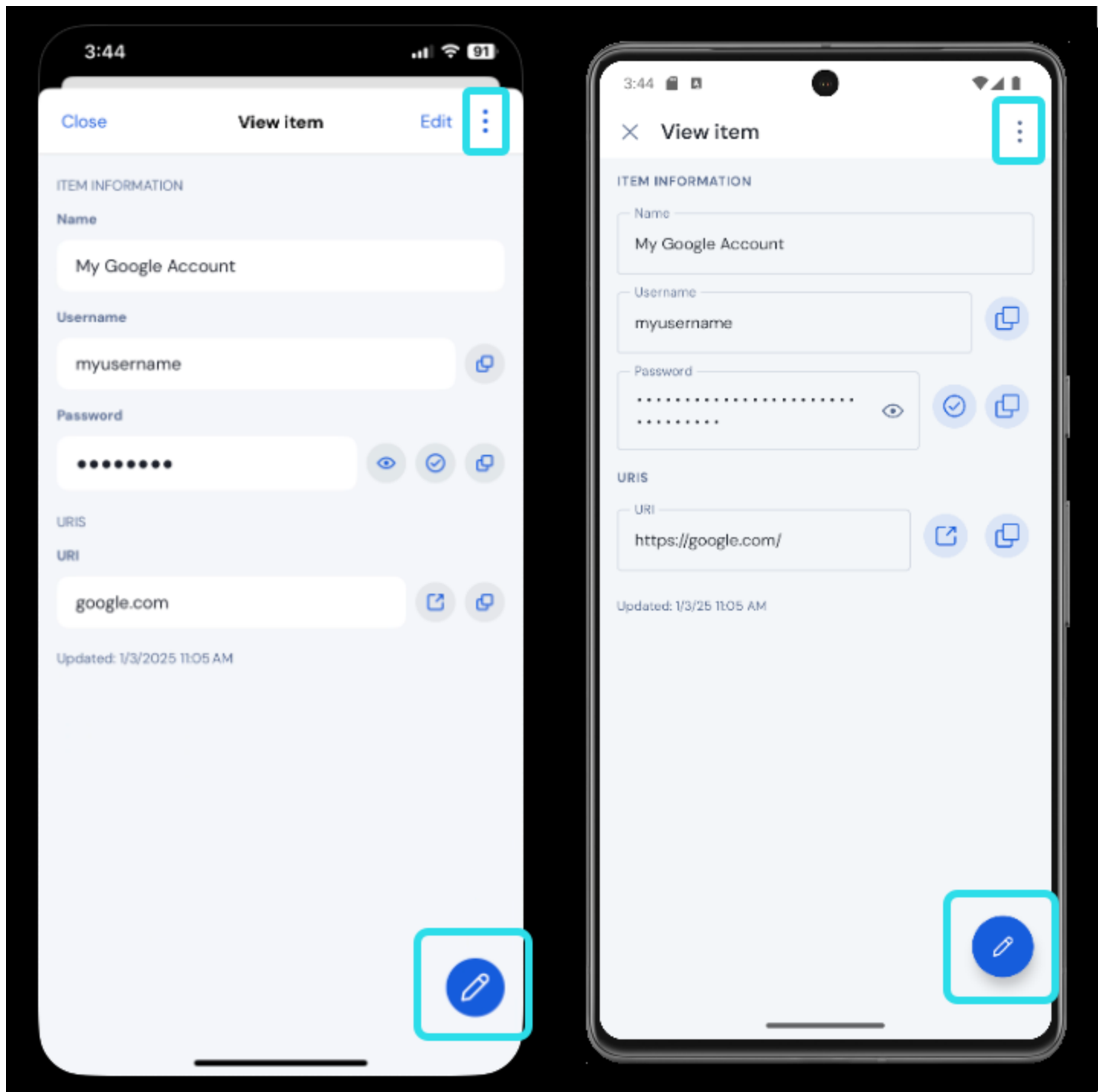
⇒Mobile

Tap an item to open it, or tap the + icon to add a new item:



Add or open an item on mobile

When viewing an item, tap the  icon to edit, or tap the  options menu to edit:



Manage an item on mobile

⇒Desktop

The screenshot shows the Bitwarden Desktop application. The sidebar on the left contains navigation options: 'ALL VAULTS', 'My vault', 'Free org', and 'My Enterprise'. Below these are 'All items', 'Favorites', and 'Trash'. Further down are 'TYPES' (Login, Card, Identity, Note, SSH key) and 'FOLDERS'. The main area displays a list of vault items: 'Credit' (Visa *1234), 'Facebook' (facebook-account123@mail.com), 'GitHub Auth' (SHA256:7o0kcCv/tih06gUSRh9Kqxp9W...), 'Id' (John Doe), 'Passport' (John Smith), and 'Reddit' (Reddit-fan-3@mail.com). The 'Facebook' item is highlighted with a red box. To the right, the details for the 'Facebook' item are shown, including login credentials (Username: facebook-account123@mail.com, Password: [masked], Verification code (TOTP): 201 729) and autofill options (Website: facebook.com). At the bottom, there are buttons for 'My vault', 'Send', '+', 'Edit', 'Share', and 'Delete'.

Manage an Item

⇒CLI

For more information, refer to the Bitwarden [CLI documentation](#).

In addition to adding, editing, and deleting vault items, you can [clone](#) items to create duplicates, [move items](#) to an organization, and [protect items](#) on an individual basis.

Clone

You can clone any item that you have ownership of if you want to create a duplicate of the item. Cloning items owned by an organization can be only done from the web app in the [Admin Console](#) or from Vaults view by owners, admins, and users with [Can manage](#) access to the collection in which the item is kept:

⇒Web app

Select **Clone** from the ⋮ **Options** menu.

⇒Browser extension

In the **Vault** tab, select the ⋮ **Options** menu for the item and choose **Clone** from the dropdown.

⇒Mobile

Open the item and tap **Clone** in the ⋮ **Menu**.

⇒Desktop

Open the item and select the **Clone Item** option.

Assign to collections

If you're a member of an [organization](#), you can assign vault items to your organization's collections, transferring ownership of the vault item to the organization. To share with other organization members, use the ⋮ menu:

The screenshot shows the Bitwarden web interface. On the left is a sidebar with 'Vaults' selected. The main area is titled 'All vaults' and contains a table of vault items. The table has columns for selection, name, icon, and owner. The 'Company Credit Card' item is highlighted with a red circle around its owner dropdown menu, which is open and shows the 'Assign to collections' option. The 'My New Item' and 'Secure Note' items are also highlighted with red boxes around their selection checkboxes. The 'Shared Login' item is also visible at the bottom.

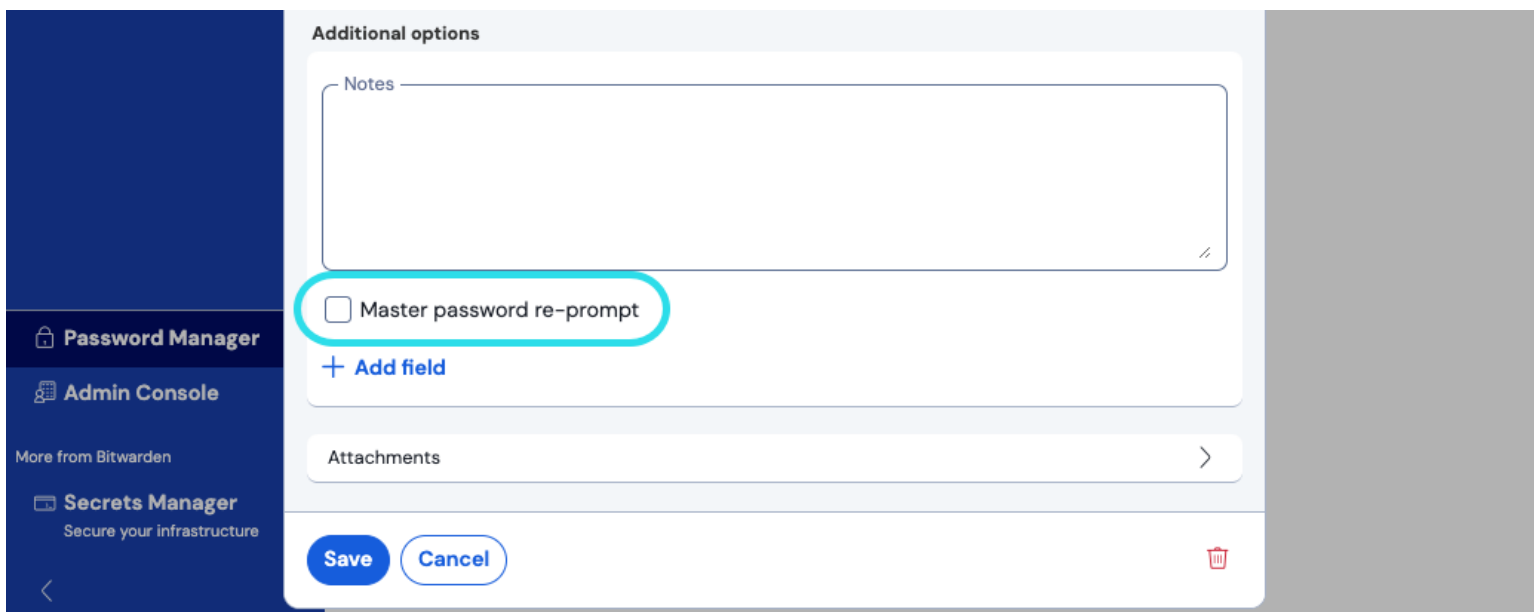
	All	Name	Owner
☐		Company Credit Card Visa, *4242	
☐		My Mailing Address Brett Warden	
☒		My New Item myusername	
☐		Personal Login myusername	
☒		Secure Note	
☐		Shared Login username	

Assign to collections

Learn more about [organizations](#), [collections](#), and [sharing](#).

Protect individual items

For any item, you can activate the **Master password re-prompt** option from the Add or Edit screen to require verification of your [master password](#) to access or autofill sensitive vault items:



Master password re-prompt

Master password re-prompt will behave slightly differently depending on which app you're using, for example:

- In the web app, browser extension, and desktop app viewing the item or editing anything about it with this enabled will require you to re-enter your master password.
- On mobile apps, only viewing hidden fields (e.g. passwords, hidden custom fields, credit card numbers) will require you to re-enter your master password. Editing anything about the item will also require you to re-enter your master password.

Users who do not have master passwords, for example those in organizations using [SSO with trusted devices](#) or [Key Connector](#), will have master password re-prompt disabled for them. Additionally, trusted contacts using [emergency access](#) will not be required to re-enter a master password in order to view a protected vault item.

Warning

Master password re-prompt **is not** an encryption mechanism. This feature is an interface-only guardrail that a sophisticated user may find ways to work around. We recommend **never** leaving your vault unlocked when unattended or on a shared workstation.

Vault trash

Deleted items are sent to the trash, where they remain for 30 days after deletion. Once 30 days have elapsed, the item will be permanently deleted and not recoverable.

In the trash, you can **Restore** an item to your vault or **Permanently delete** it prior to the 30-day waiting period using the  menu:

⇒Web app

Select **Trash** from the Filters menu:

Password Manager

Vaults

Send

Tools

Reports

Settings

Filters

Search trash

All vaults

My vault

My Organization

New organization

All items

Favorites

Login

Warning

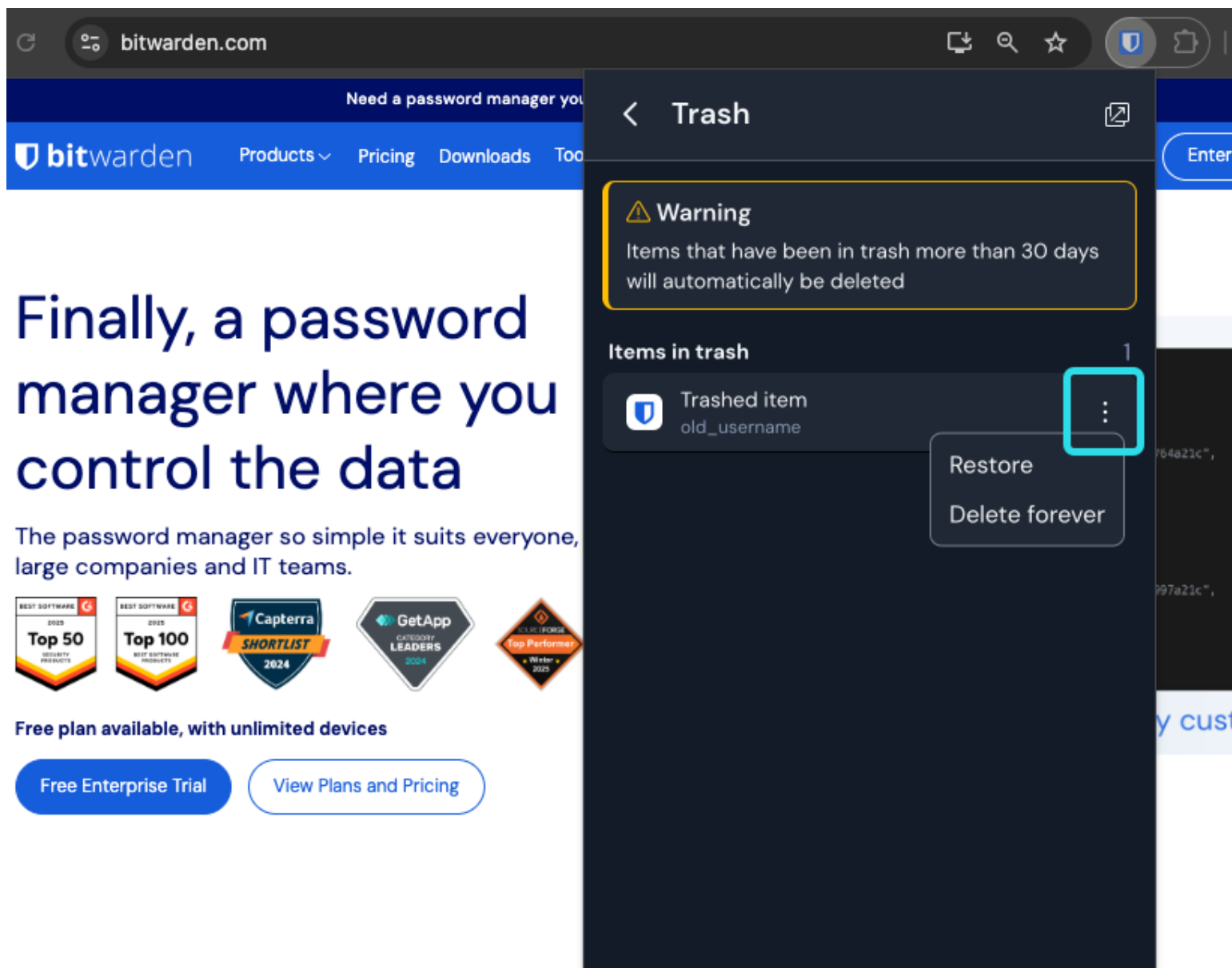
Items that have been in trash more than 30 days will be automatically deleted.

All	Name	Owner	
☐	Trashed Item	Me	Attachments Restore Permanently delete

Trash in the web app

⇒Browser extension

Navigate to **Settings** → **Vault** → **Trash**:

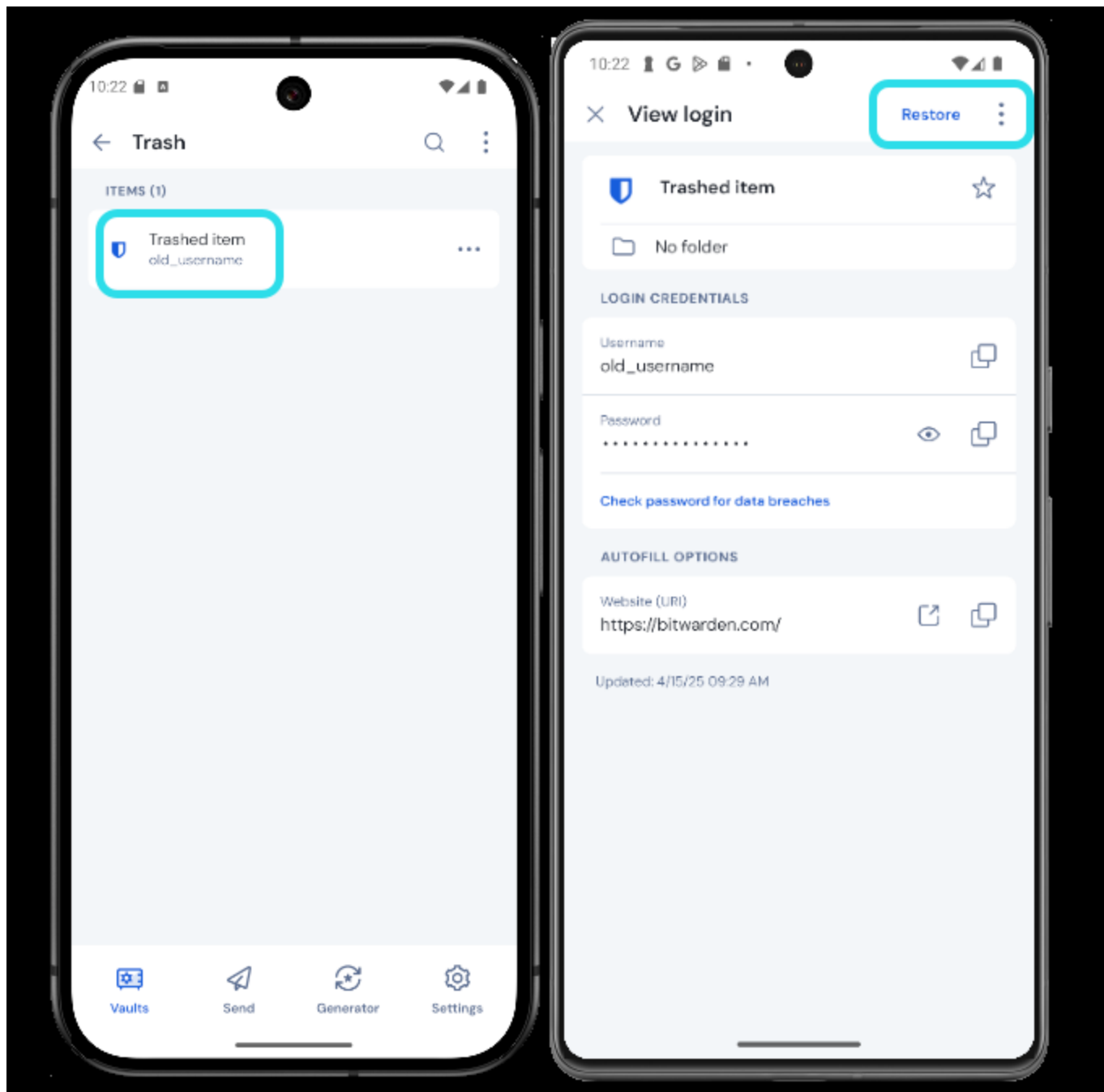


The image shows a composite of two screenshots. On the left is the Bitwarden website homepage, featuring the company logo, navigation links (Products, Pricing, Downloads, Tools), and a main headline: "Finally, a password manager where you control the data". Below this, it states "The password manager so simple it suits everyone, large companies and IT teams." and lists several awards from Capterra, GetApp, and others. At the bottom, there are buttons for "Free Enterprise Trial" and "View Plans and Pricing". On the right is a screenshot of the Bitwarden browser extension's "Trash" interface. It shows a warning message: "Warning: Items that have been in trash more than 30 days will automatically be deleted". Below this, there is a list of "Items in trash" with one item: "Trashed item old_username". A red box highlights the three-dot menu icon next to this item, which has opened a context menu with two options: "Restore" and "Delete forever".

Trash in browser extensions

⇒ Mobile app

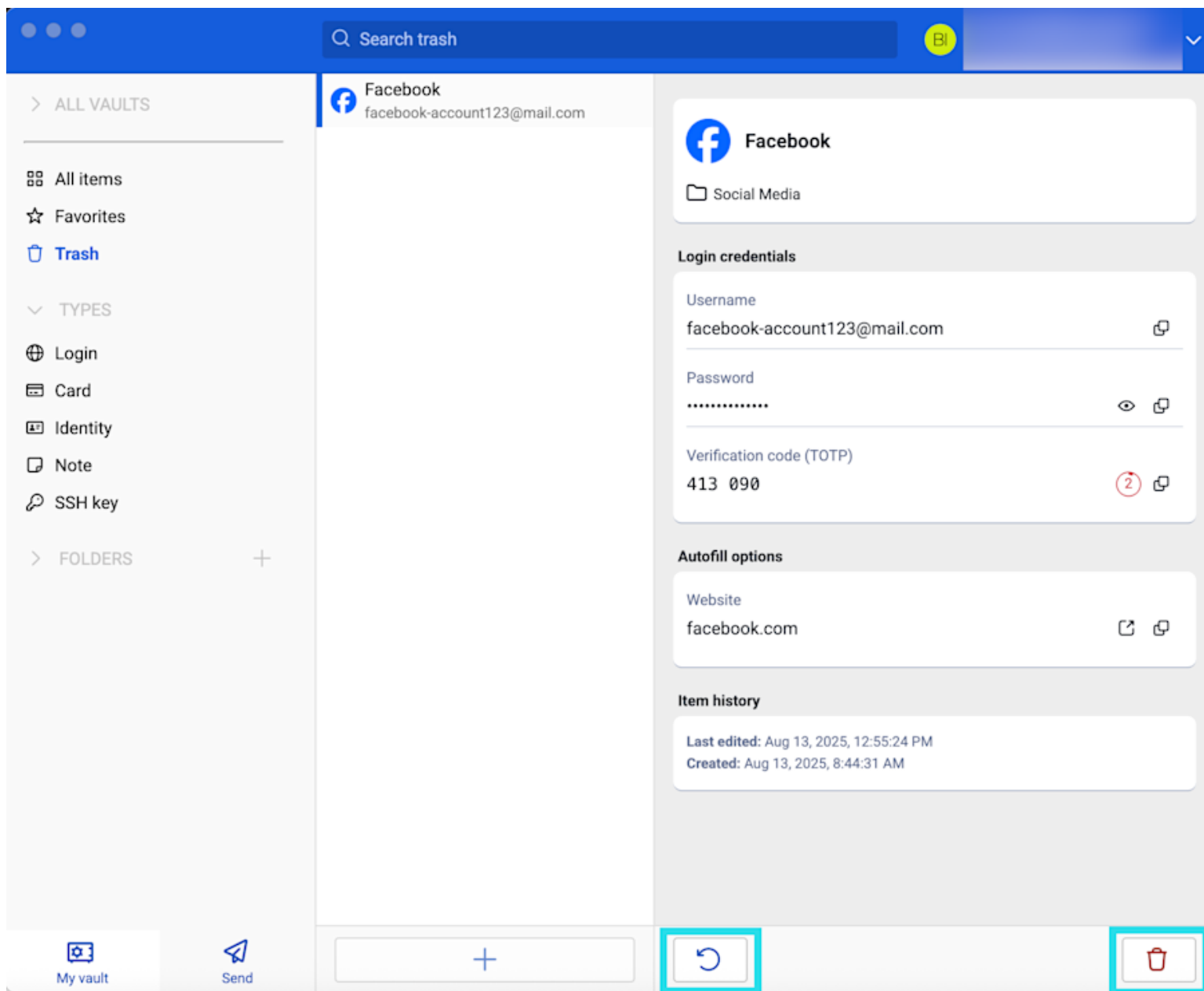
On the **Vaults** tab, scroll down to **Trash** and select the item:



Trash in mobile apps

⇒Desktop app

Select **Trash** from the navigation:



Trash in desktop apps

Next steps

Now that you understand the basics of working with vault items, we recommend:

- Organizing your vault item using [favorites](#) and [folders](#)
- Adding [custom fields](#), [TOTP seeds](#), and [file attachments](#) to vault items