

PASSWORD MANAGER > VAULT BASICS

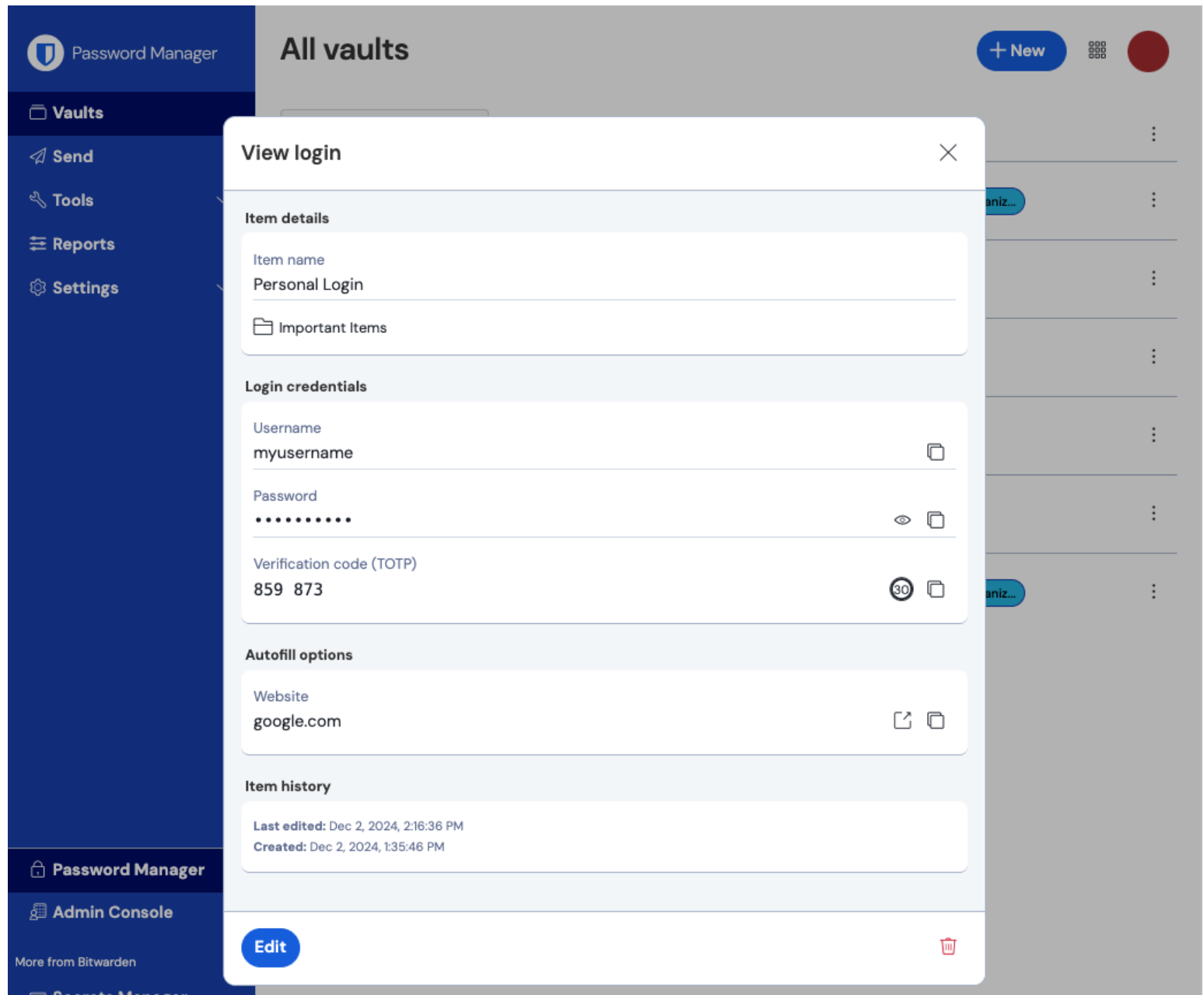
Vault Items

Vault Items

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

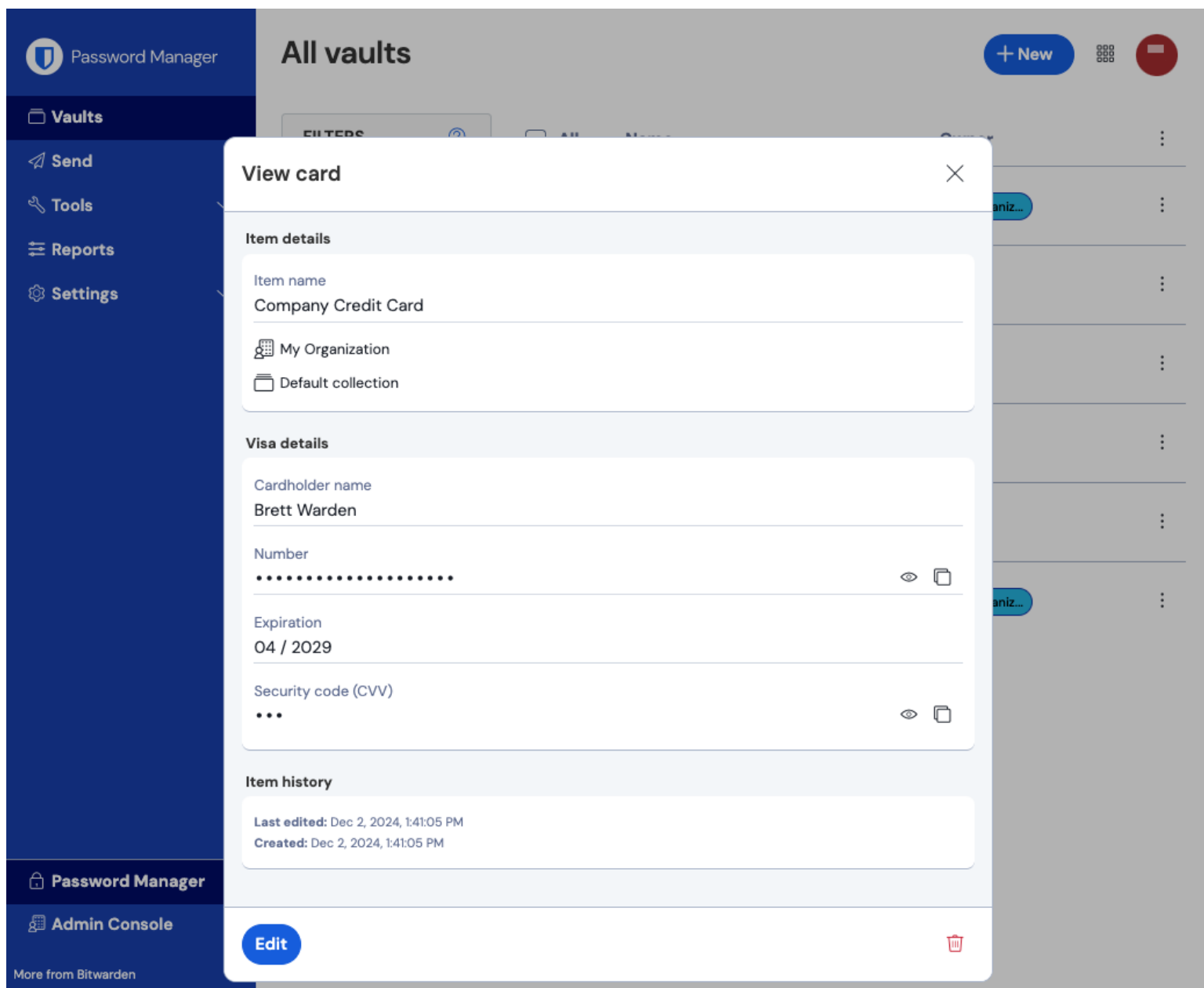
Logins are most often used to store username and password combinations, passkeys, and support [TOTP seeds](#) for premium users. Whatever plan you are on, we recommend giving every login a [URI for easy autofill](#):



Login item

⇒Cards

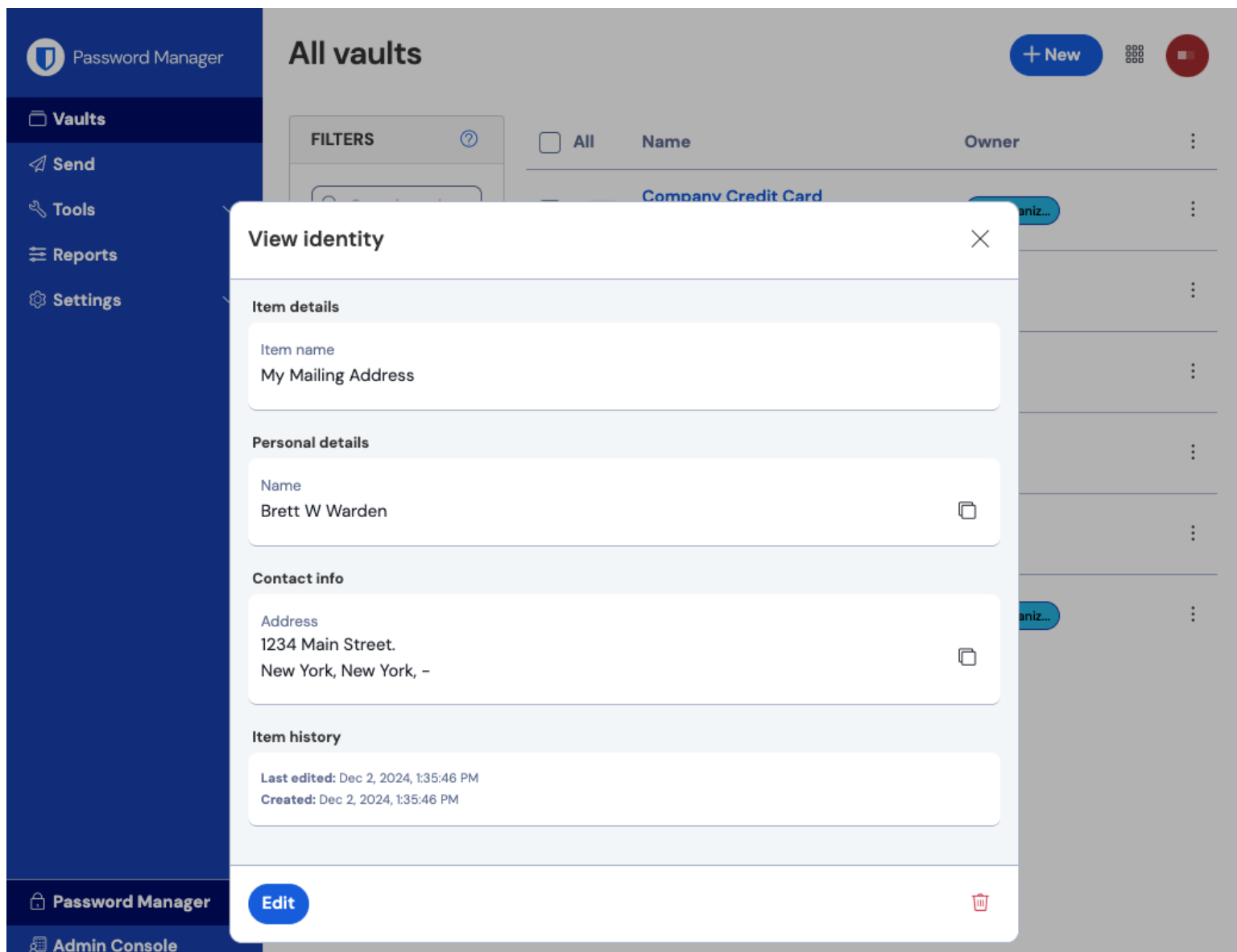
Cards can be used to securely store credit or debit card information:



Card item

⇒Identities

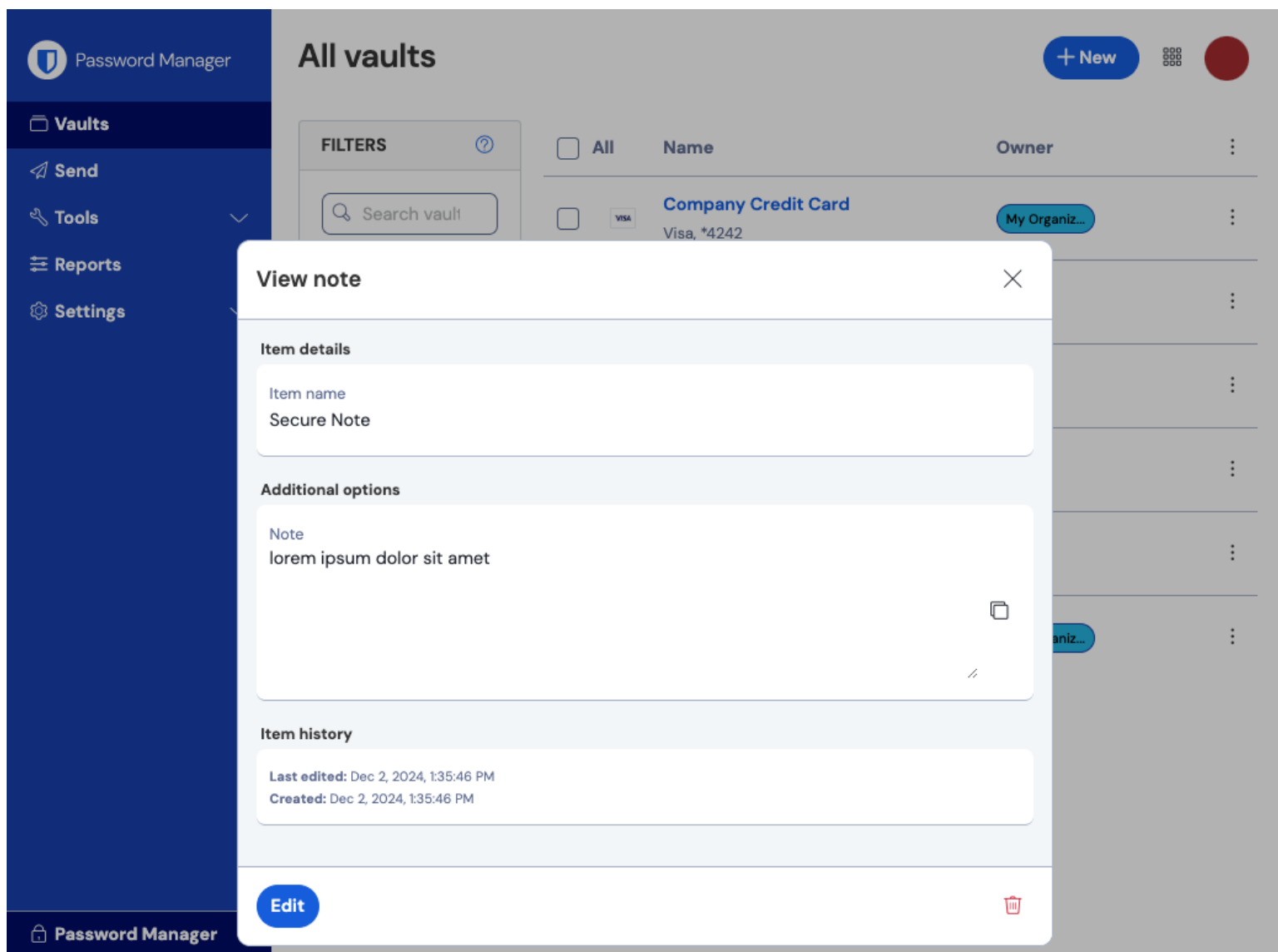
Identities can be used to store billing, mailing, and most other types of information you might need when filling out online forms:



Identity item

⇒Secure notes

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



The screenshot shows the Bitwarden web application interface. On the left is a dark blue sidebar with navigation links: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main area is titled 'All vaults' and contains a table of vaults. A modal window titled 'View note' is open, displaying details for a 'Secure Note' item. The modal includes sections for 'Item details' (showing the item name 'Secure Note'), 'Additional options' (showing a note with placeholder text 'lorem ipsum dolor sit amet'), and 'Item history' (showing 'Last edited' and 'Created' timestamps). At the bottom of the modal are 'Edit' and delete buttons. The background shows a vault named 'Company Credit Card' with a Visa card number.

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

<https://player.vimeo.com/video/823390347>

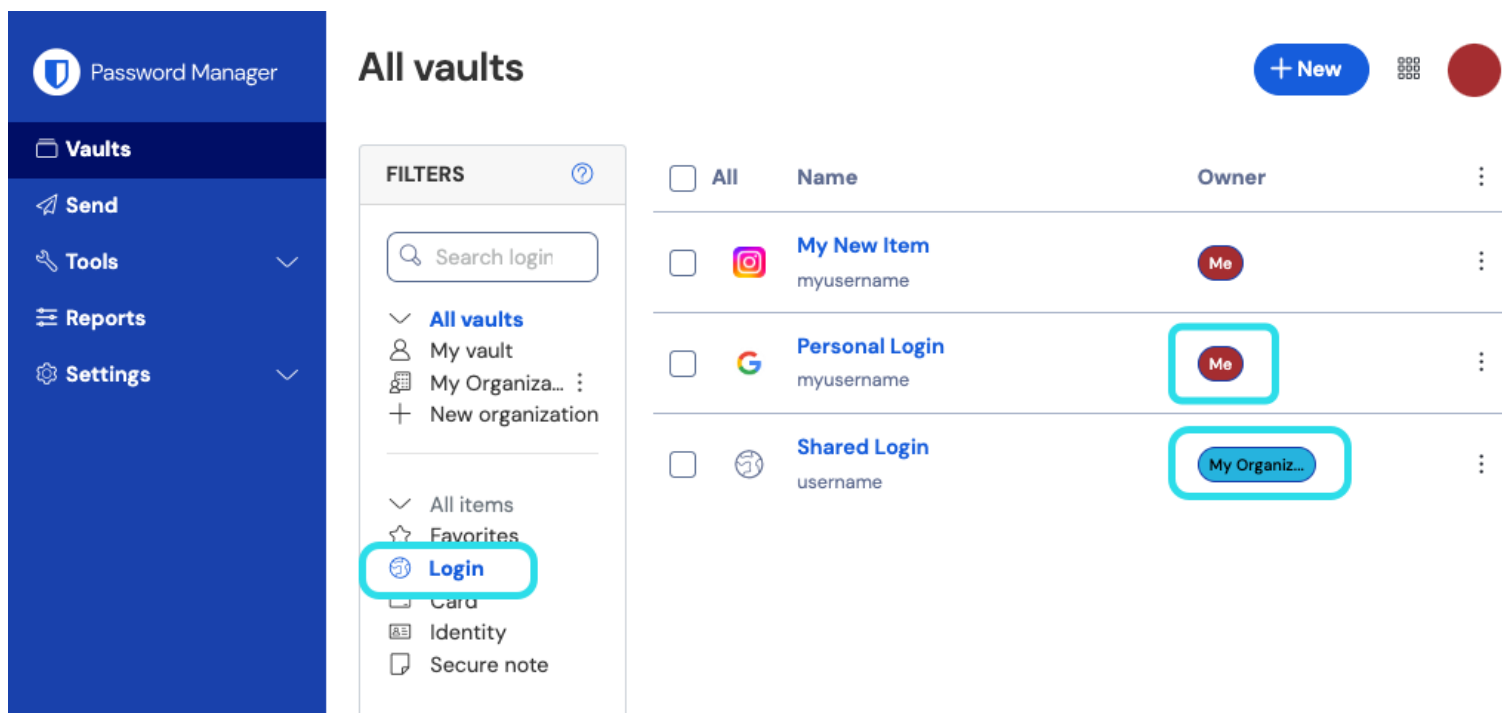
Filter vault items

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

⇒ Web app

Either:

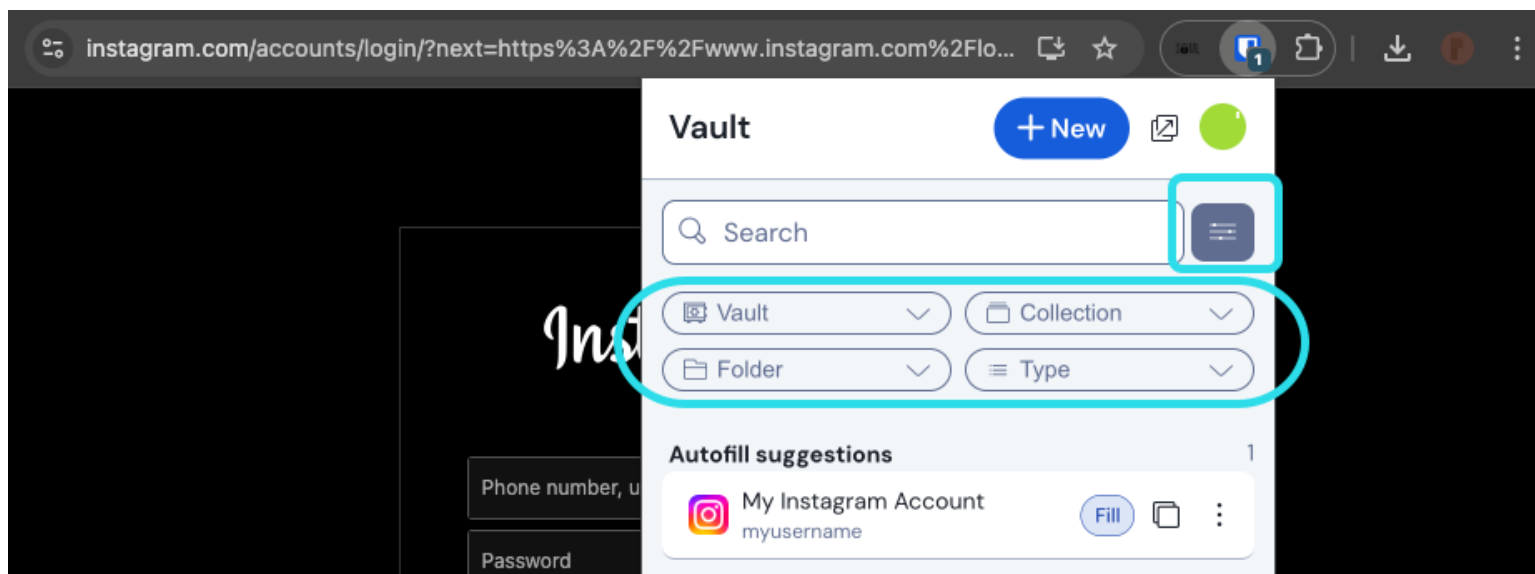
- Select a characteristic from the **Filter** column (in the following screenshot, **Login**).
- Select one of the colored cards next to an item (in the following screenshot, either **Me** or **My Organization**).



Web app filtering

⇒Browser extension

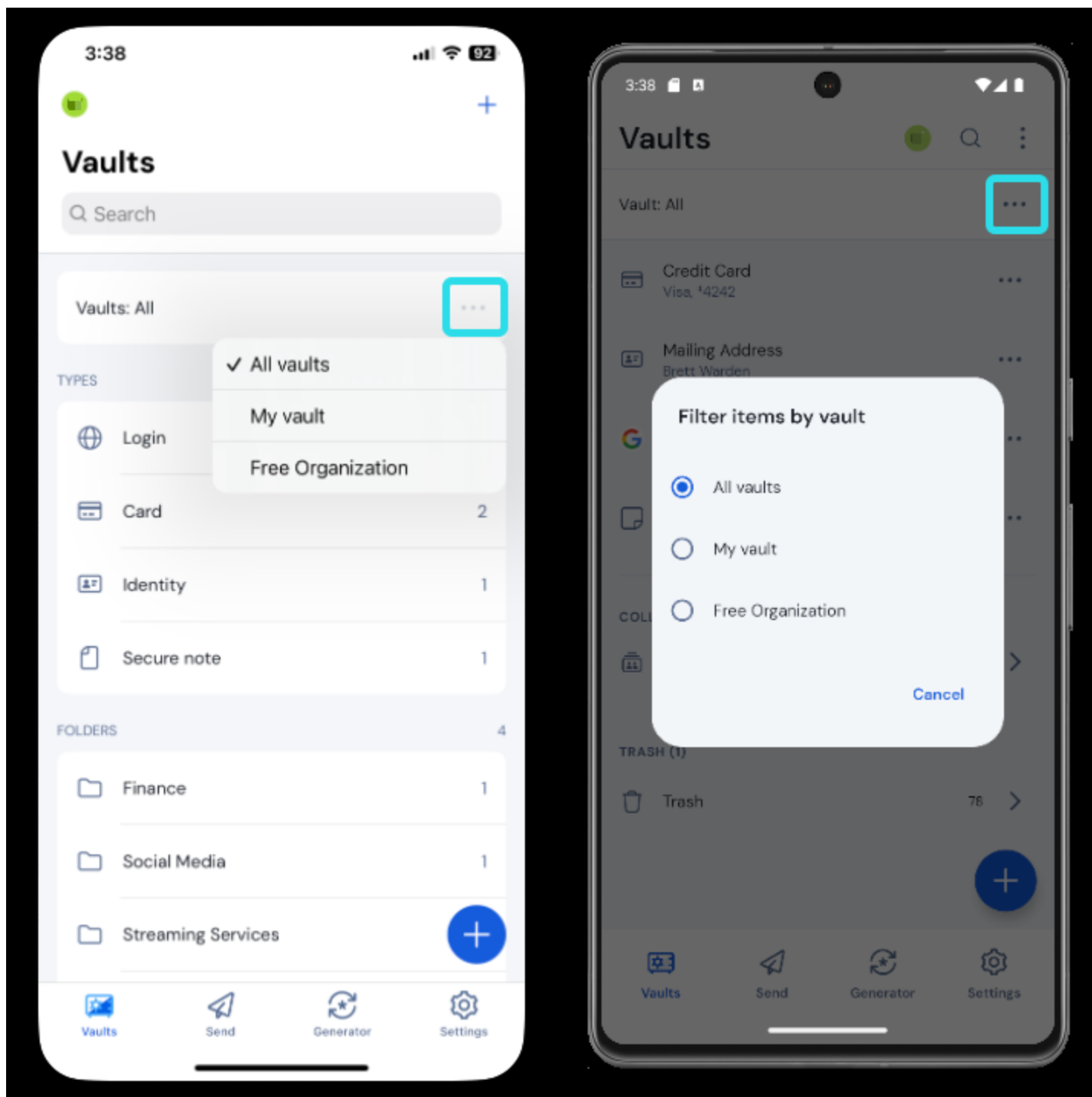
Use the **Vault**, **Collection**, **Folder**, or **Type** selectors at the top of the **Vault** tab. You can turn show and hide the filter dropdown menus with the button:



Browseruitbreiding automatisch invullen

⇒Mobile

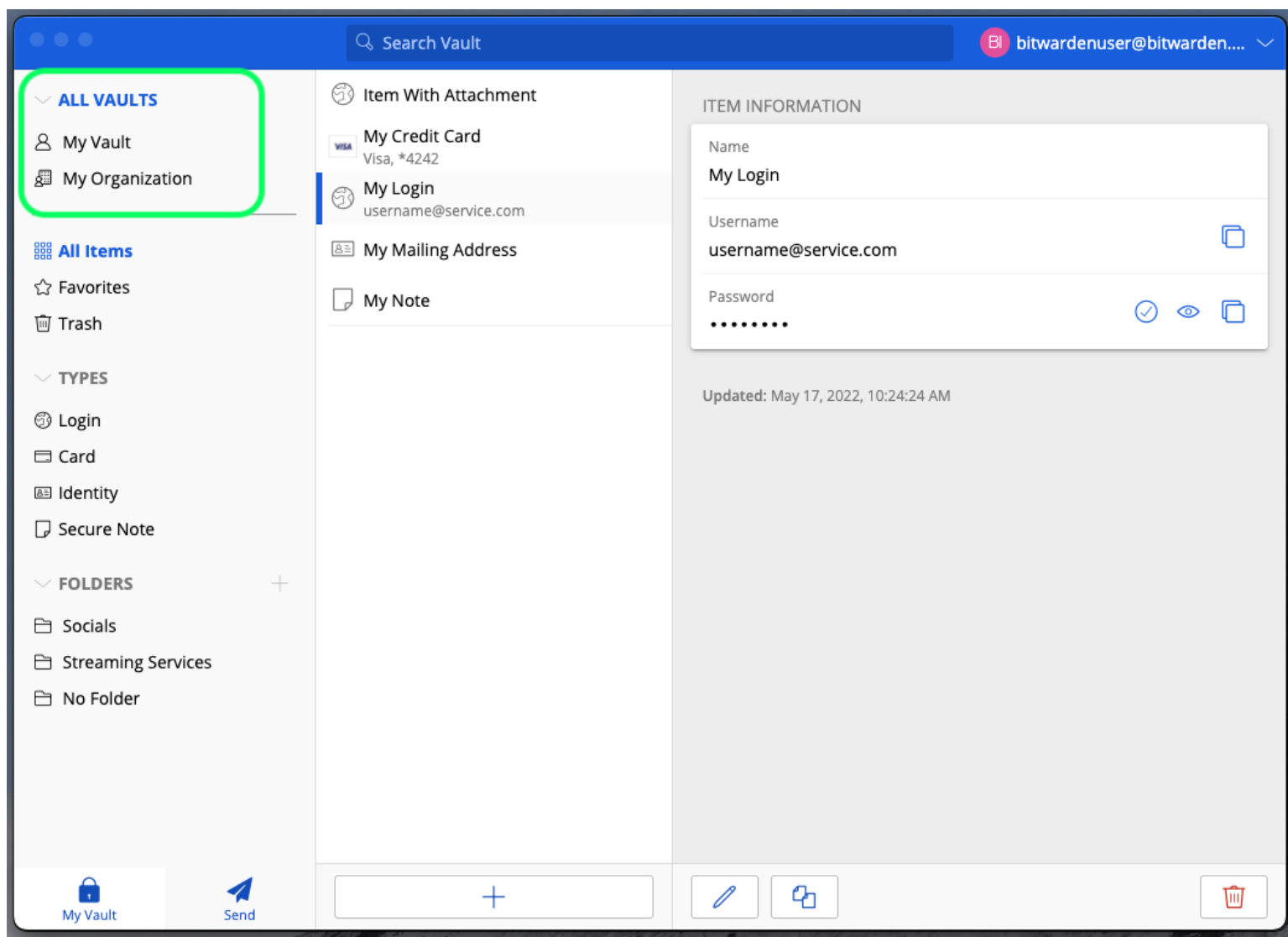
Choose a vault by selecting the **Vault** menu button () on the **Vaults** tab:



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

+ New

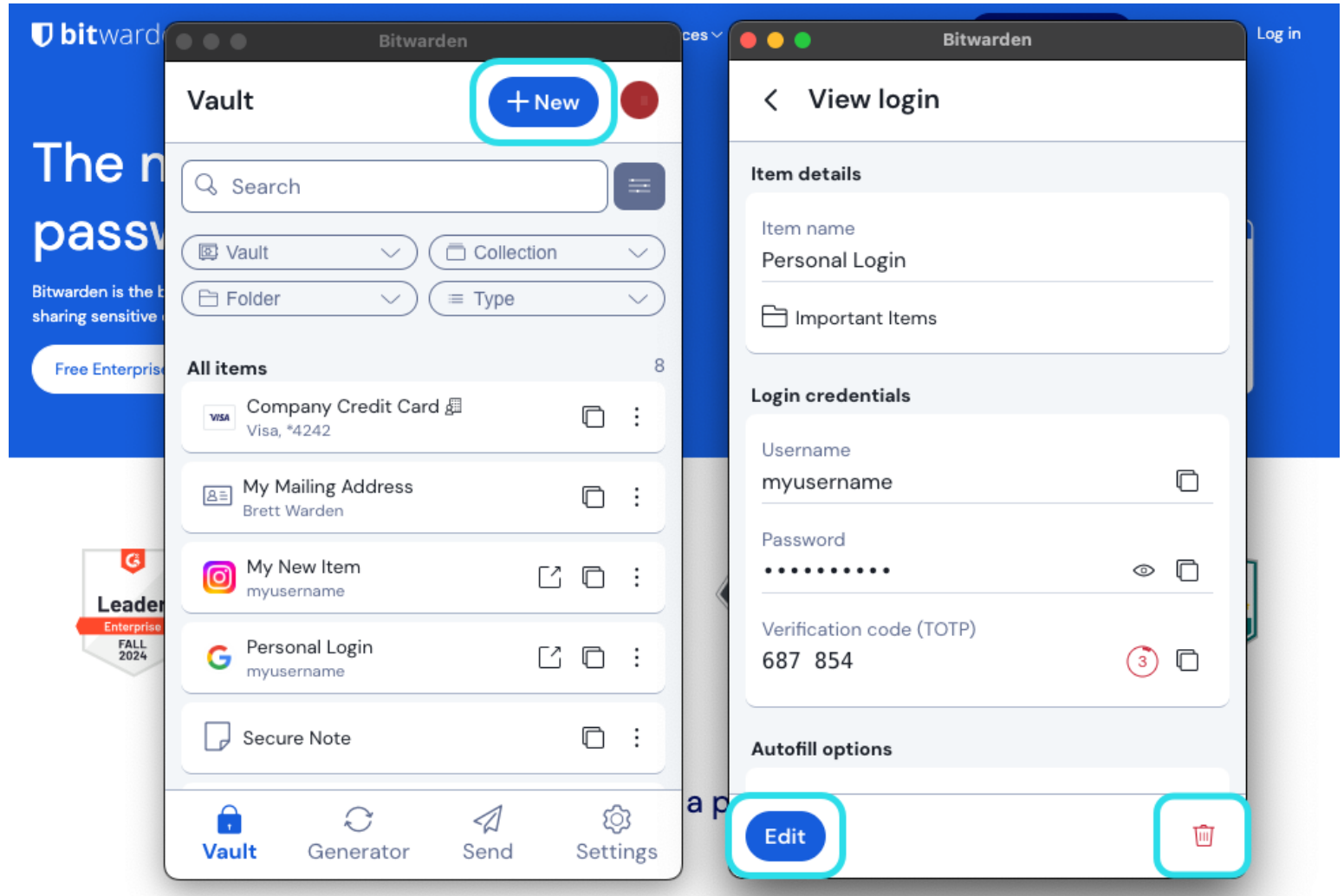
FR

	All	Name	Owner	
☐		Company Credit Card Visa, *4242	My Organiz...	
☐		My Mailing Address Brett Warden	Me	
☐		My New Item myusername	M	Attachments Clone Assign to collections Delete
☐		Personal Login myusername	N	
☐		Secure Note	Me	
☐		Shared Login username		

Once you open an item, select **Edit**.

Manage an Item

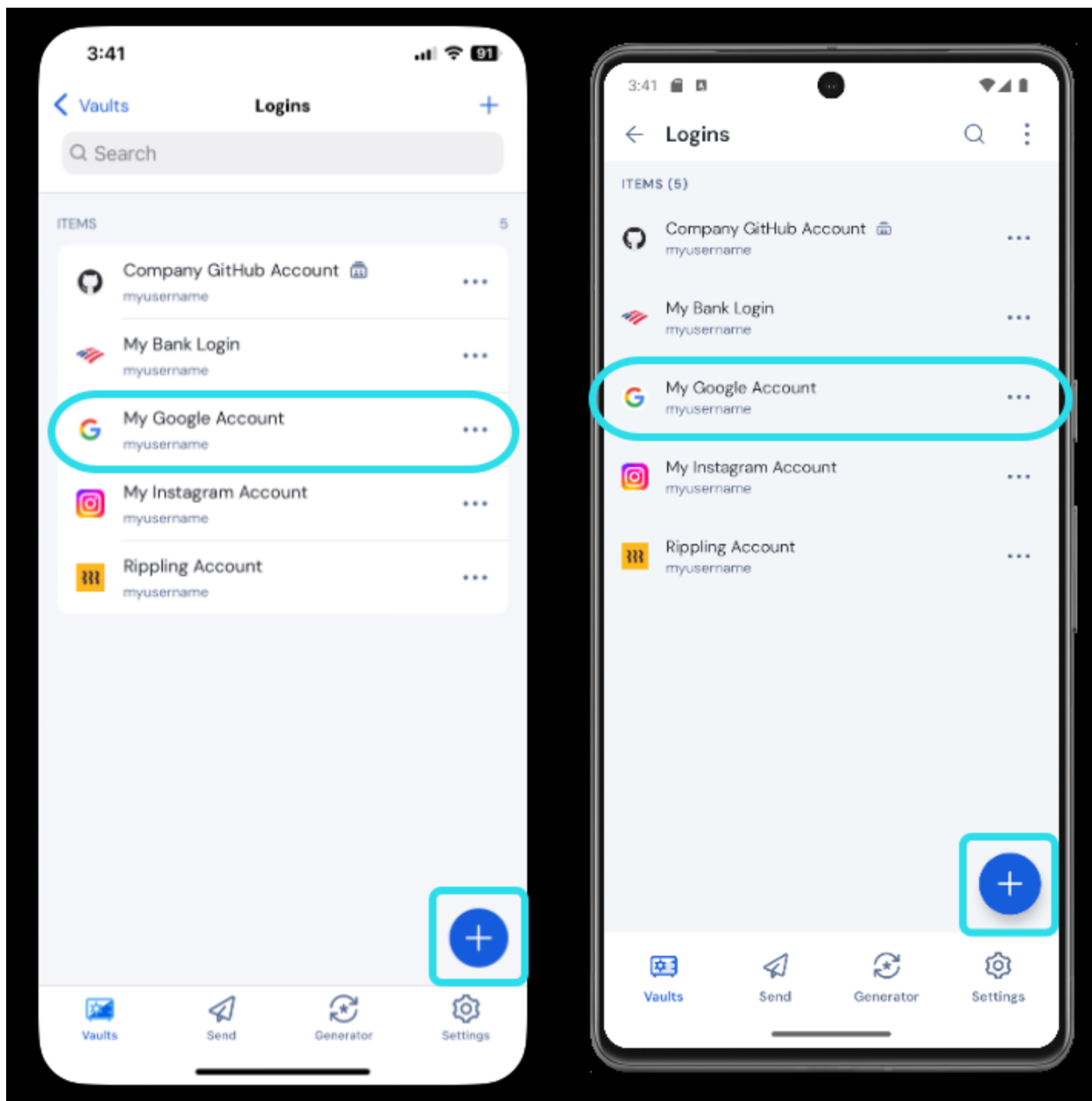
⇒Browser extensions



Manage an item

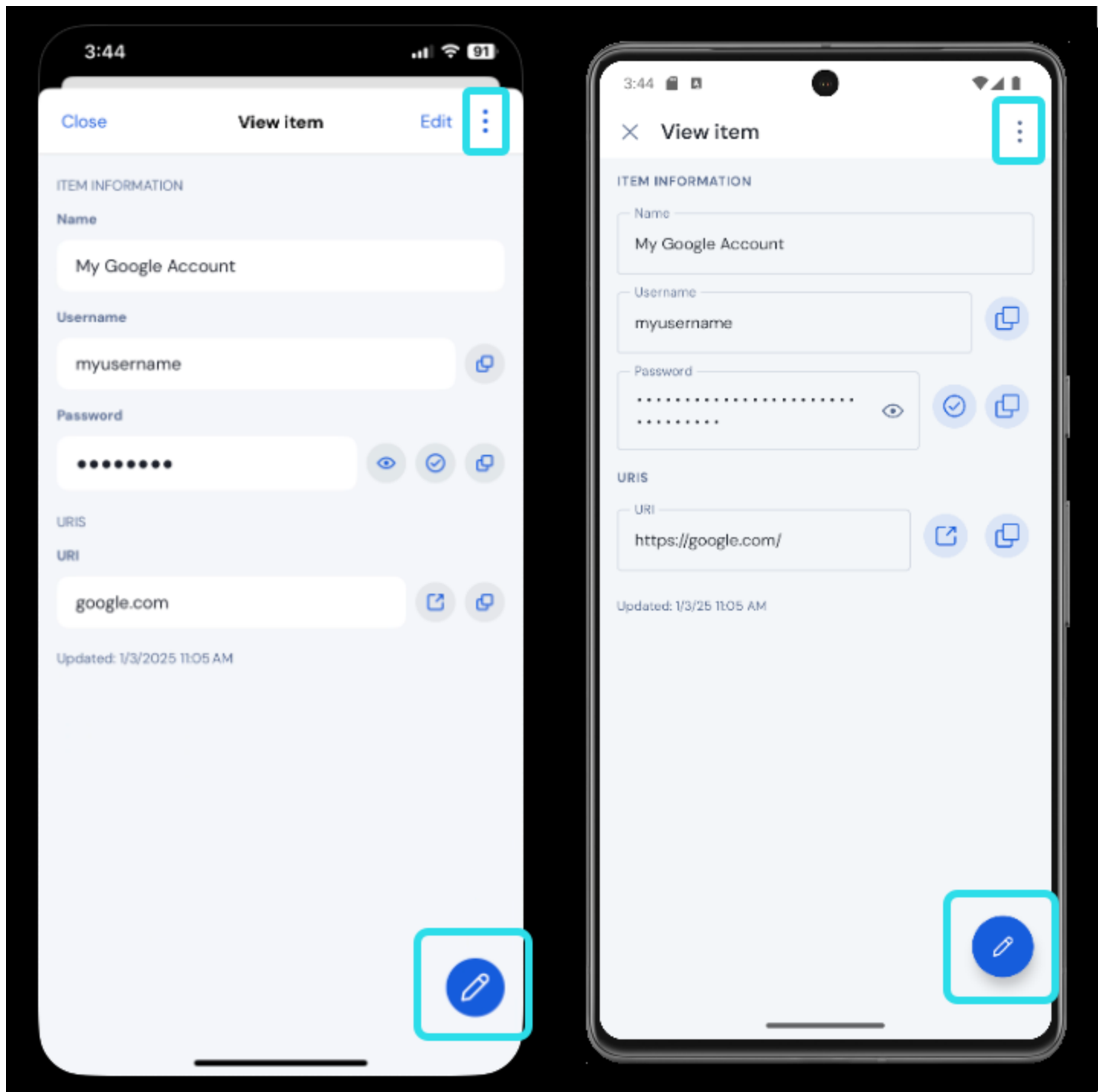
⇒Mobile

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



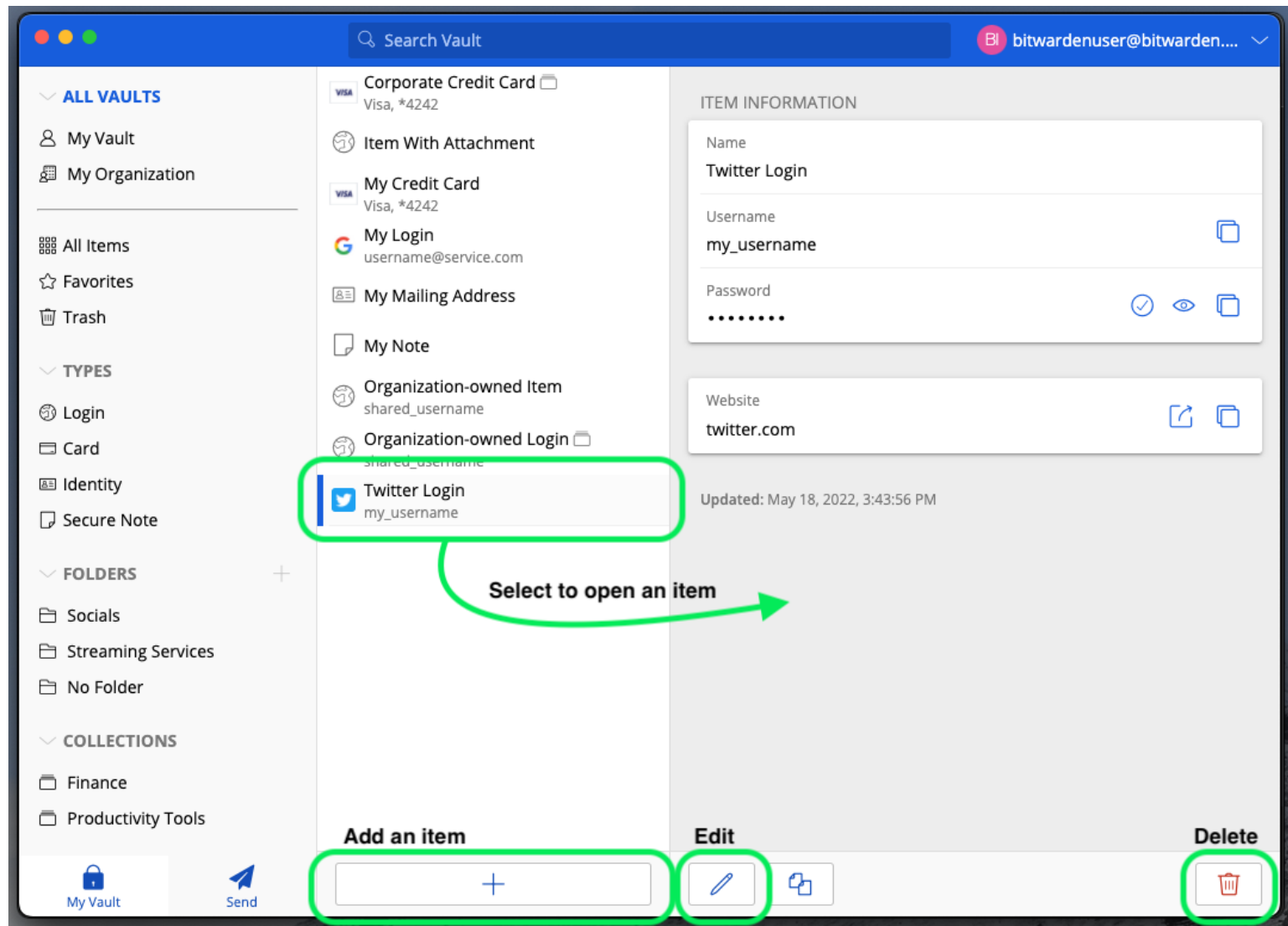
Add or open an item on mobile

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



Manage an item on mobile

⇒Desktop



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:

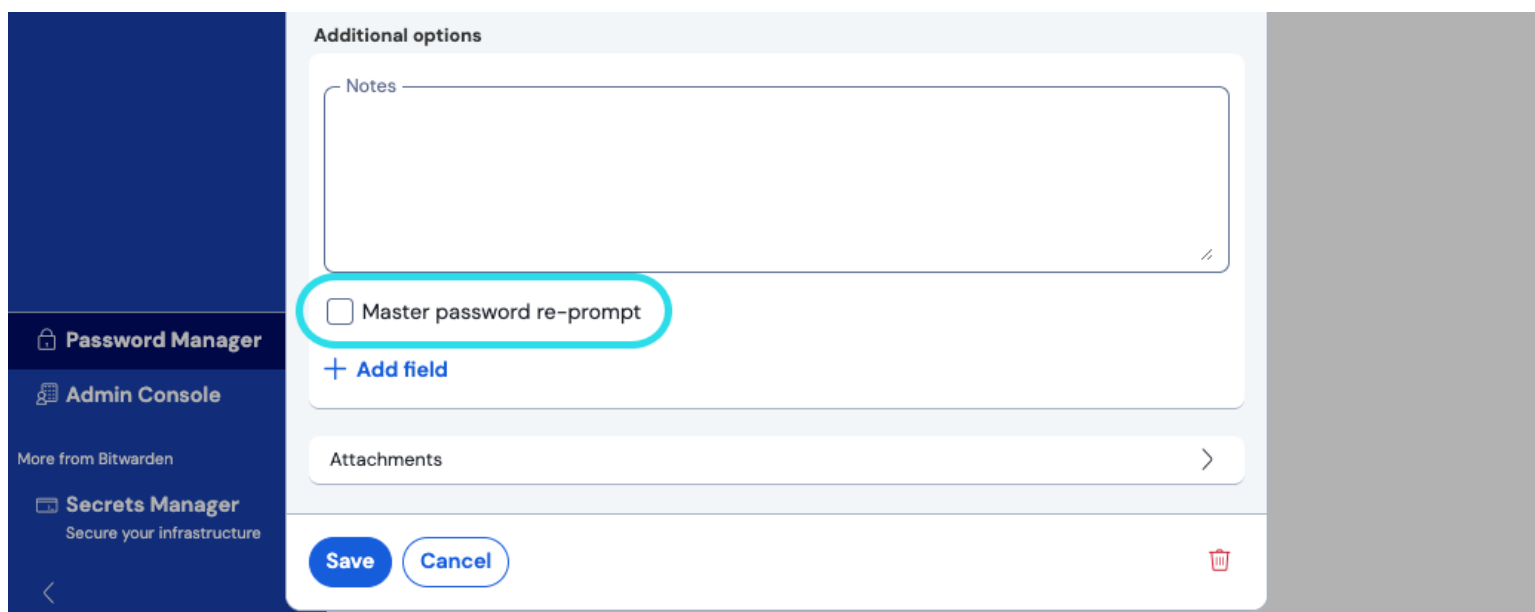
The screenshot shows the Bitwarden 'All vaults' interface. On the left is a sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main area is titled 'All vaults' and contains a list of vault items. A 'FILTERS' sidebar on the left allows searching and filtering by vault type (All vaults, My vault, My Organization, New organization) and item type (All items, Favorites, Login, Card, Identity, Secure note). The vault list includes items like 'Company Credit Card', 'My Mailing Address', 'My New Item', 'Personal Login', 'Secure Note', and 'Shared Login'. For 'My New Item' and 'Secure Note', the checkbox is checked. A dropdown menu is open for the 'My New Item' row, showing options: 'Add to folder', 'Assign to collections' (highlighted with a red circle), and 'Delete'. The 'Owner' column shows 'Me' for most items, while 'Shared Login' is owned by 'My Organiz...'. A red circle highlights the menu icon for the 'Shared Login' item.

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 and browser extension, viewing the item or editing anything about it with this enabled will require you to re-enter your master password.
- On desktop apps, and 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

All vaults

FILTERS

▼ All vaults

My vault

My Organiza...

+ 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	⋮
		old_username		

Attachments

Restore

Permanently delete

Trash in the web app

⇒Browser extension

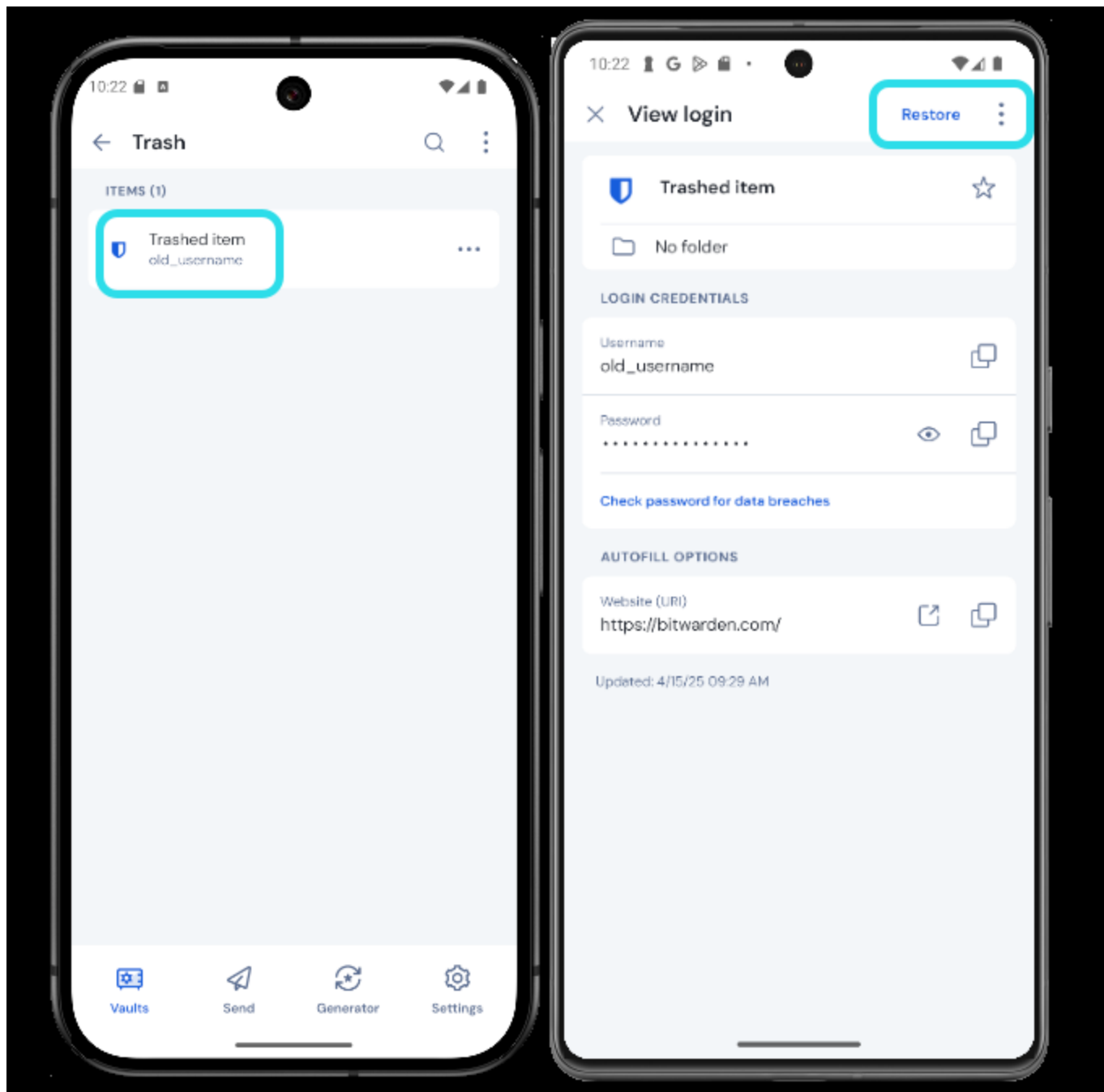
Navigate to **Settings** → **Vault** → **Trash**:

The image shows a composite of two screenshots. On the left is the Bitwarden website homepage, featuring the logo, navigation links (Products, Pricing, Downloads, Tools), and a large 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 mobile app interface showing the "Trash" section. A warning message at the top states: "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 a count of 1. The item listed is "Trashed item old_username". A red box highlights the three-dot menu icon next to the item, which has opened a context menu with two options: "Restore" and "Delete forever".

Trash in browser extensions

⇒Mobile app

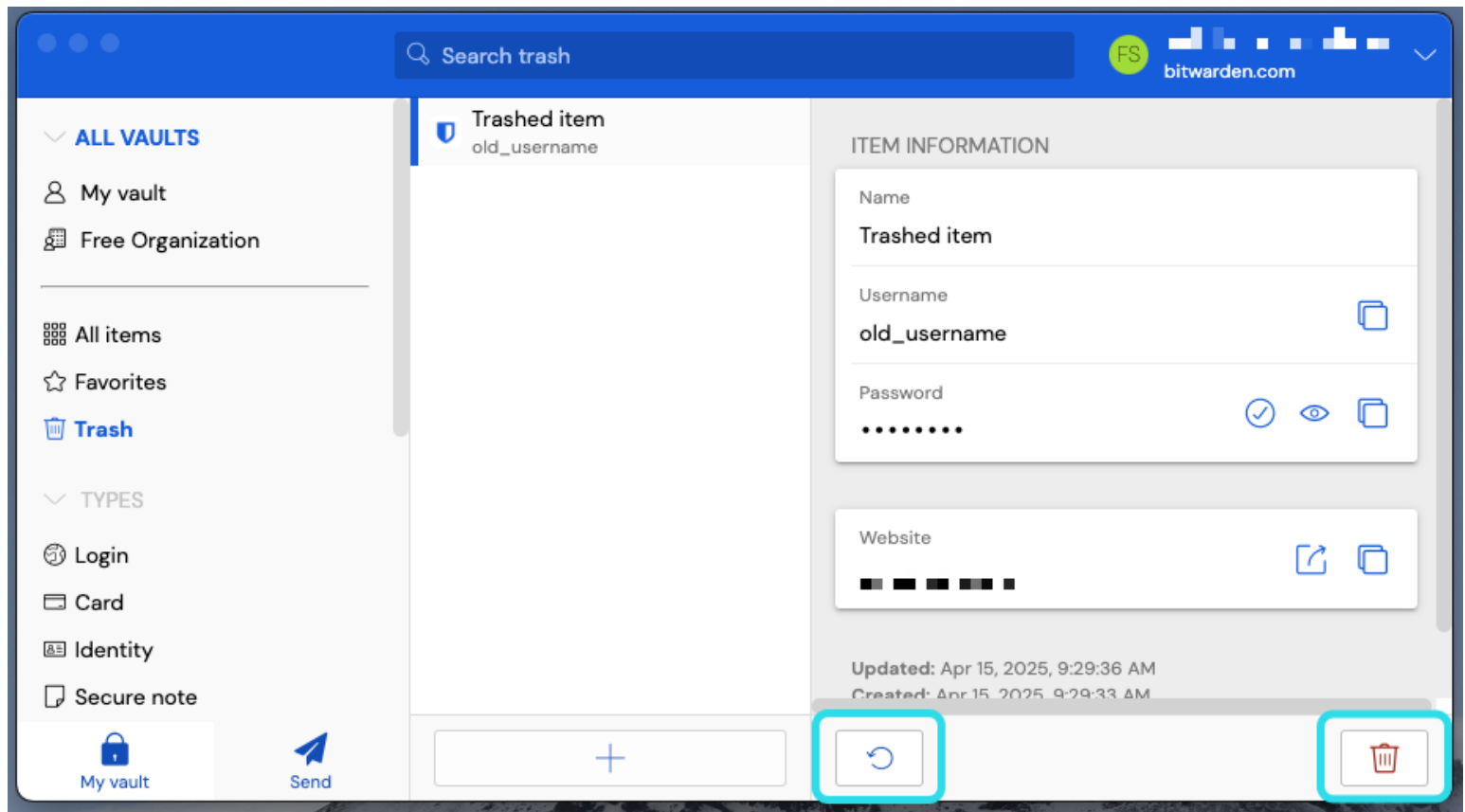
On the **Vaults** tab, scroll down to **Trash** and select the item:



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