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:
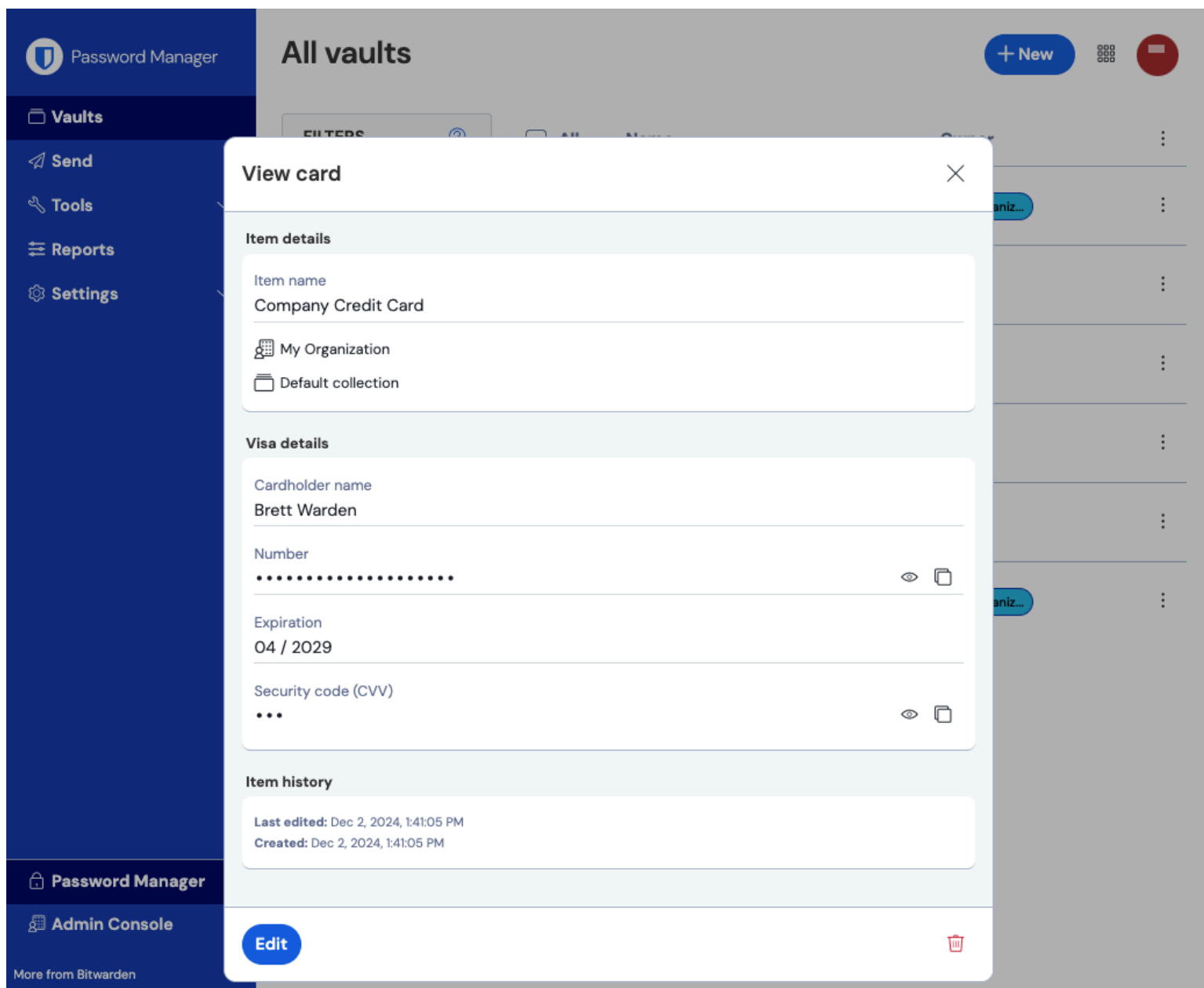
⇒Logins

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:
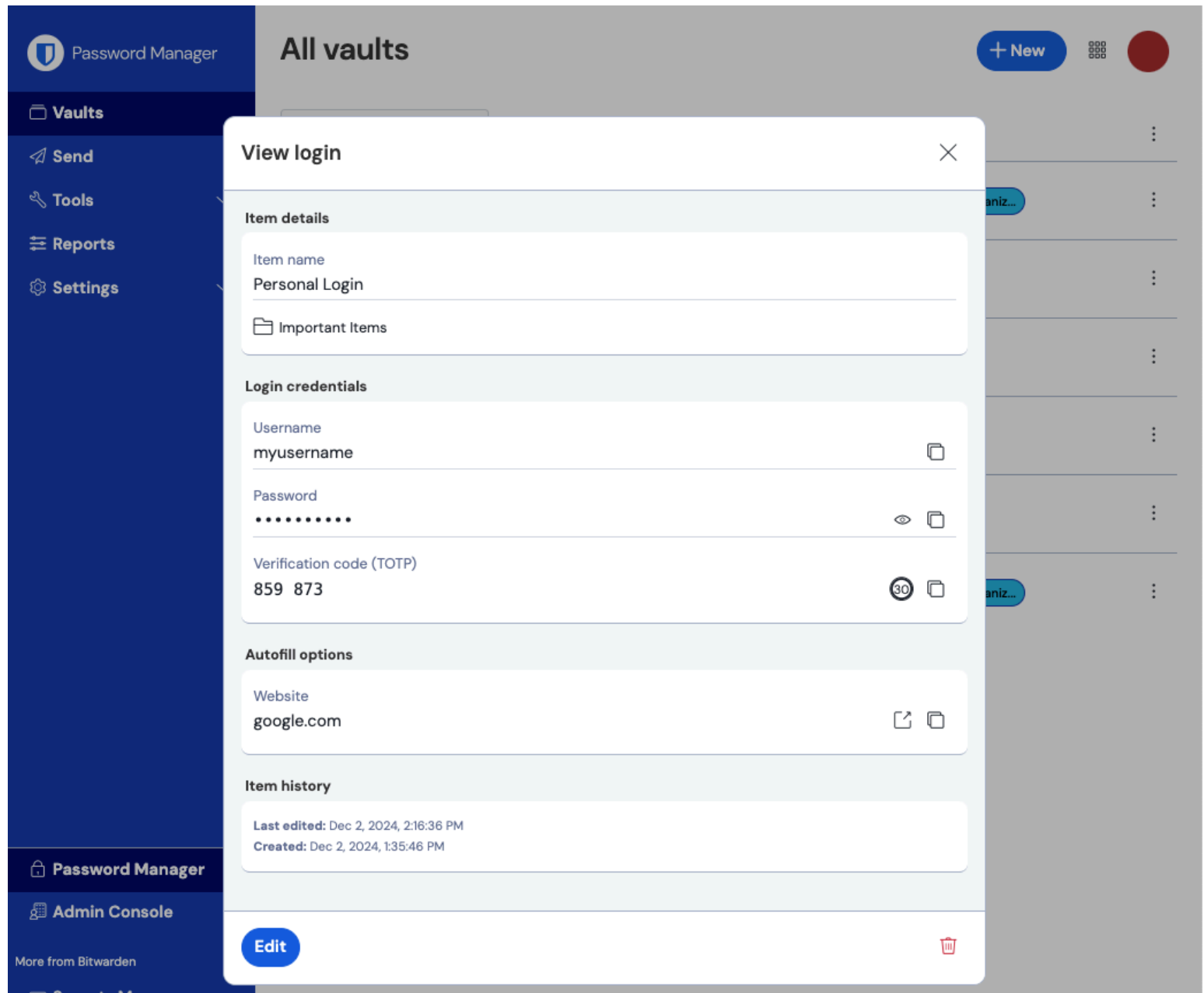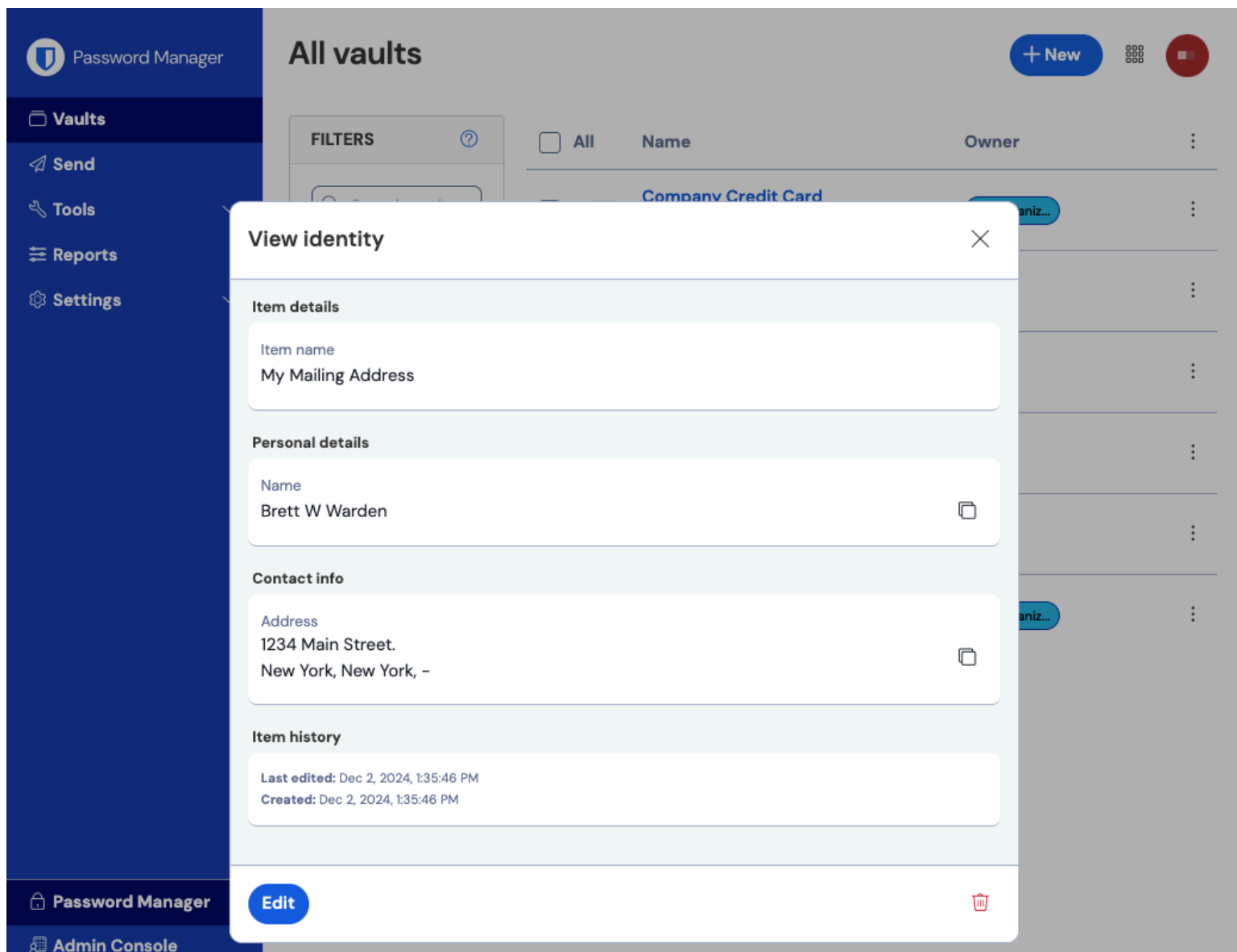

Login item

⇒Cards

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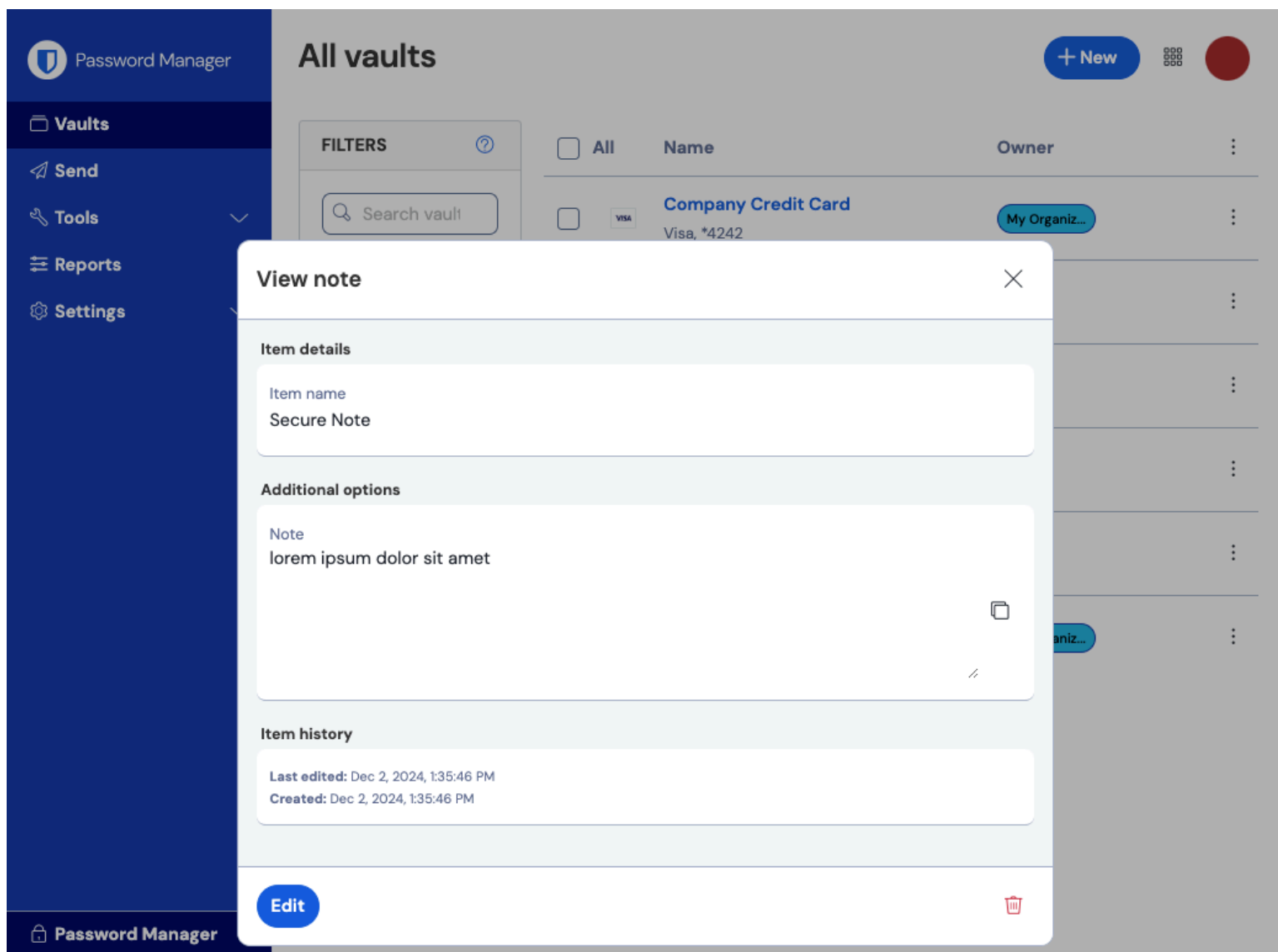
Card item

⇒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:

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:

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**).

![Bitwarden logo] **bit**warden   Secure and trusted open source password manager for business
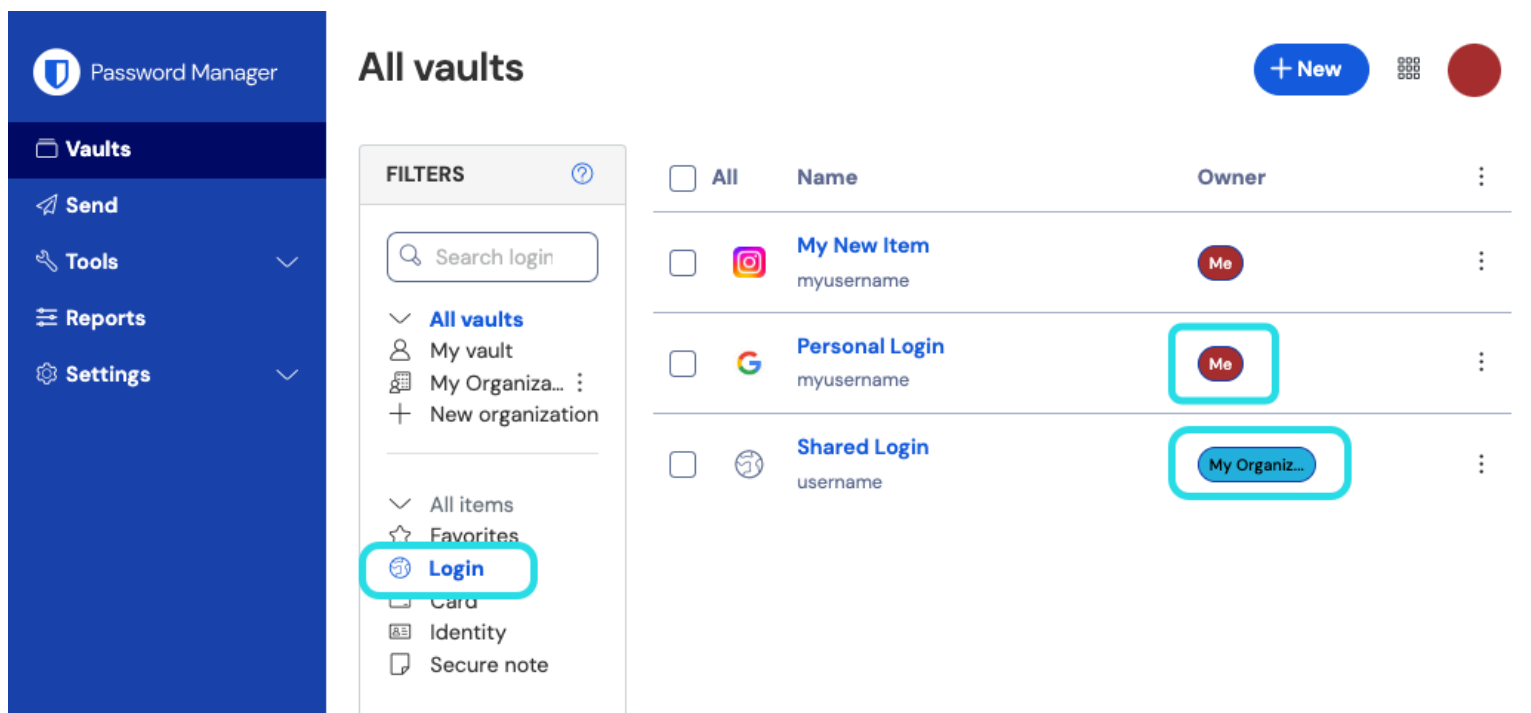
Web app filtering
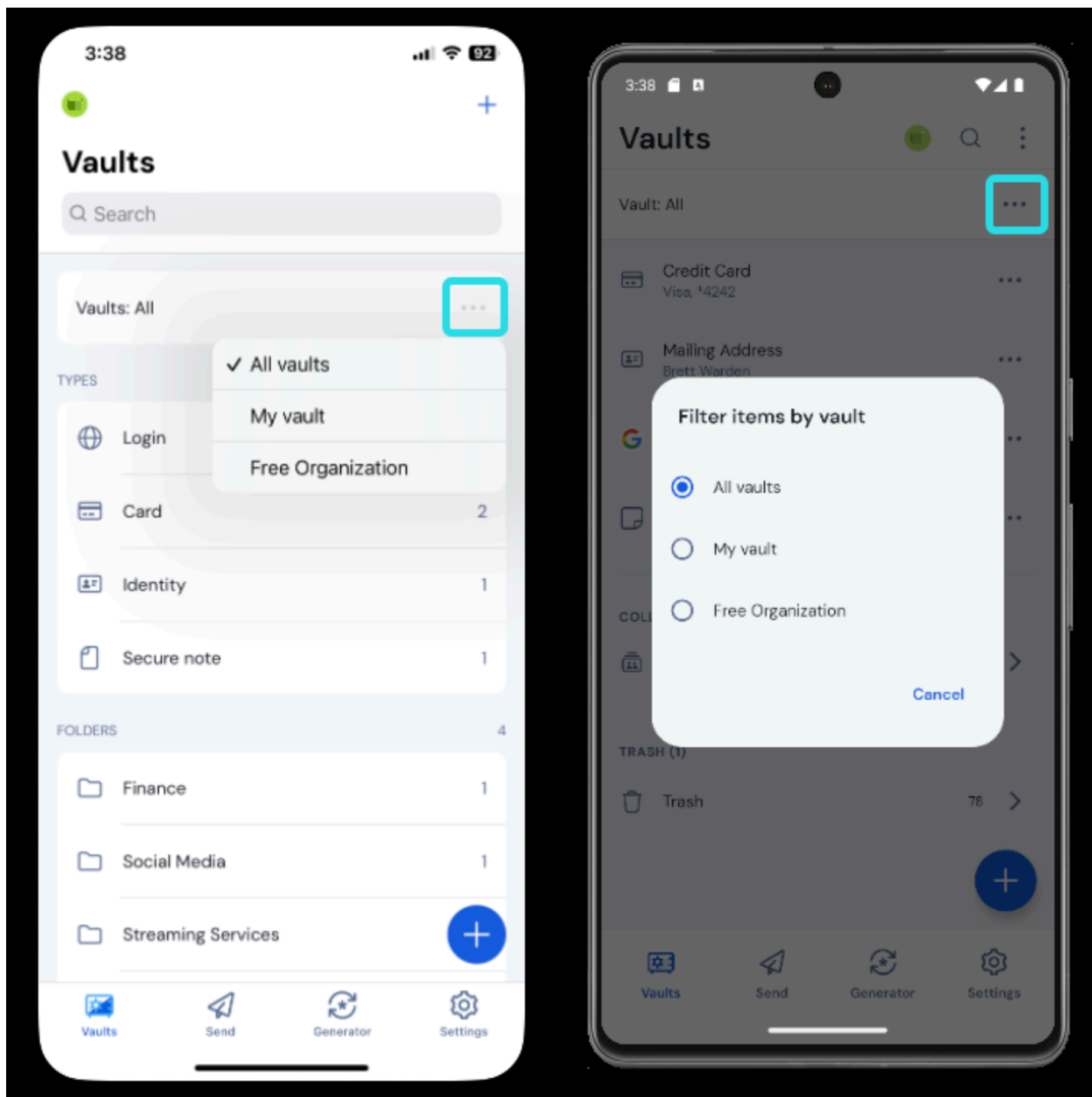
⇒Browser extension

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:
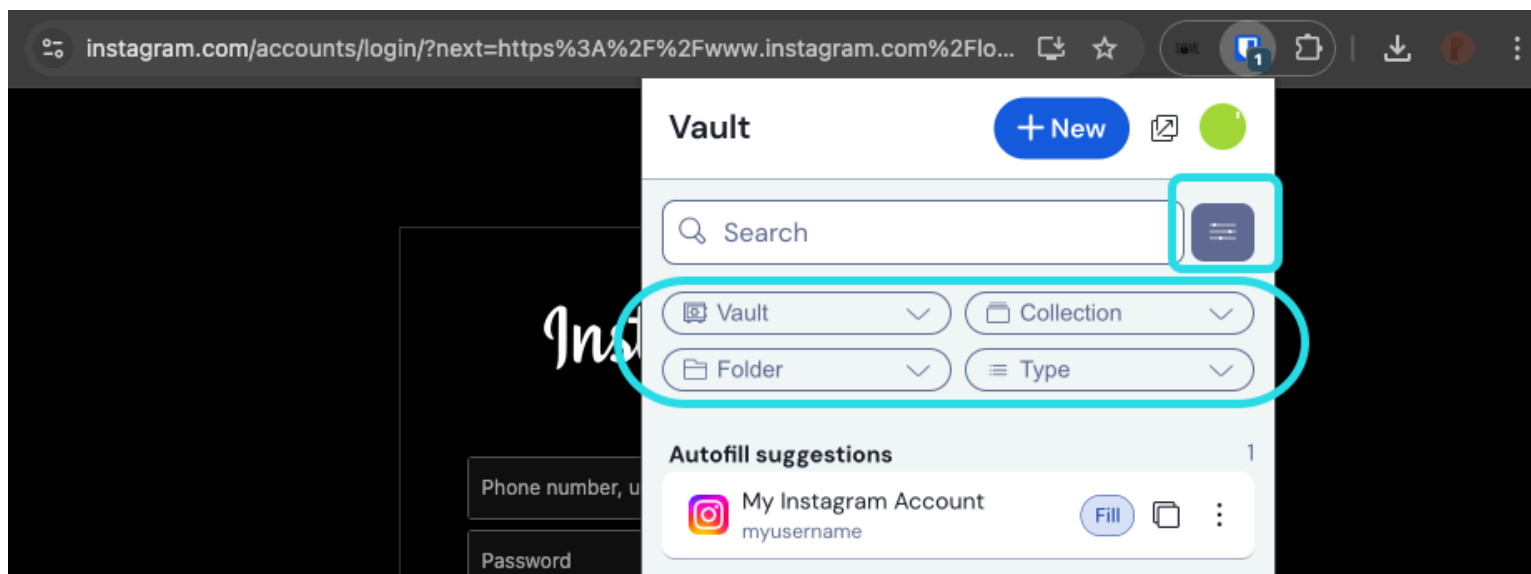
Extensión de Navegador Autocompletar

⇒Mobile

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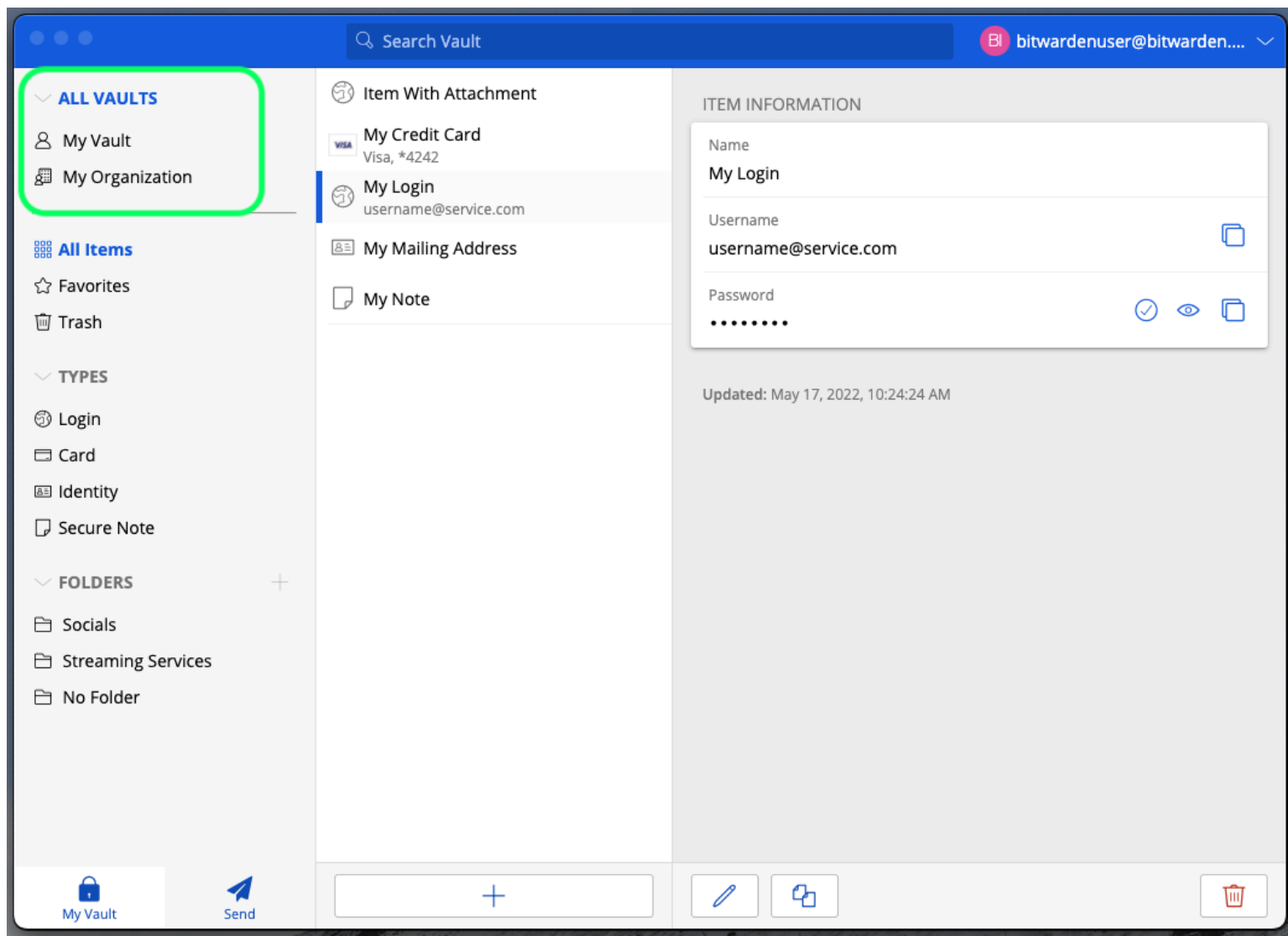
Filter vaults on mobile

⇒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:

⬛ **bit**warden

Secure and trusted open source password manager for business

⇒**Web app**

Manage an Item

⇒**Browser extensions**
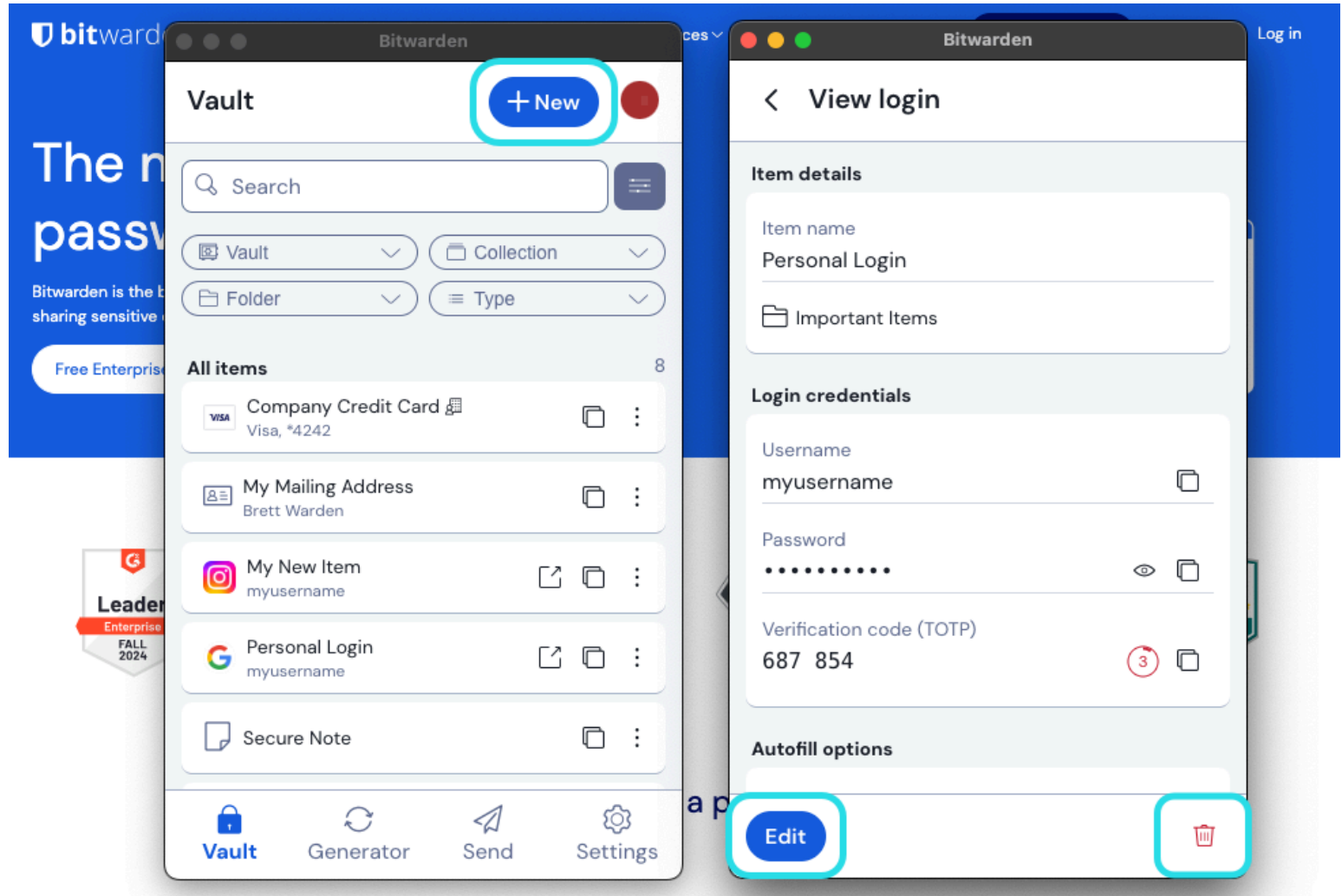
Manage an item

⇒**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:
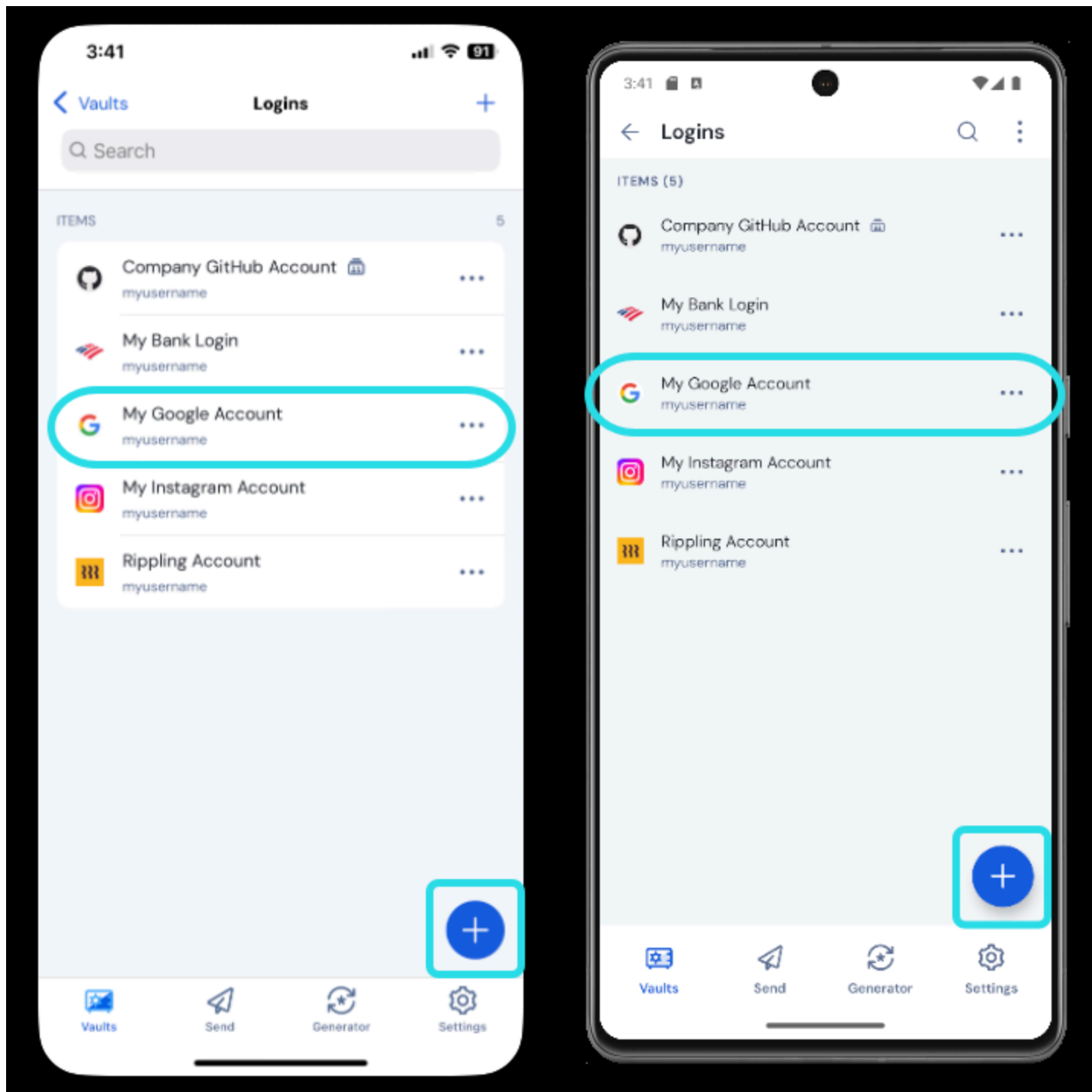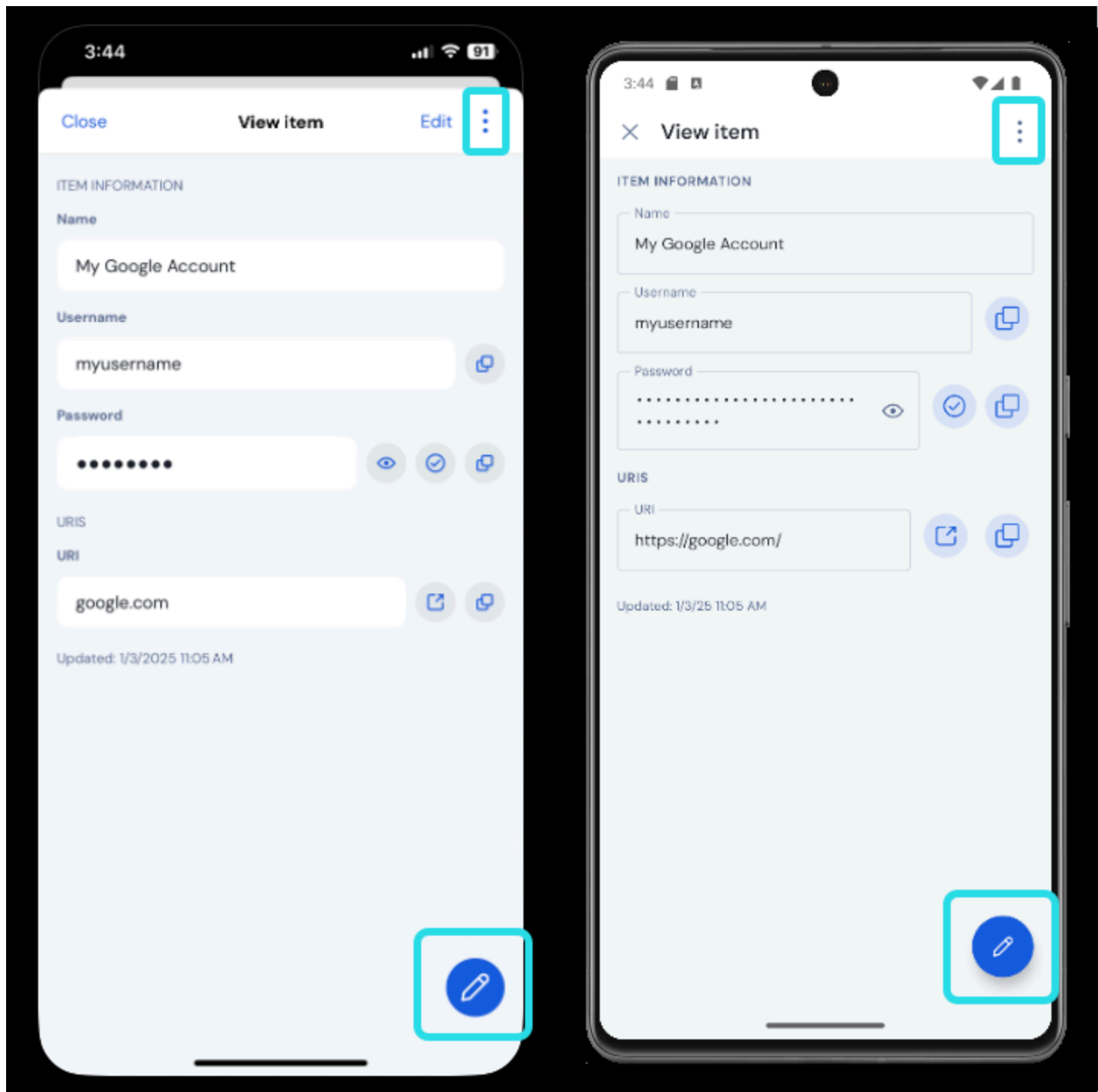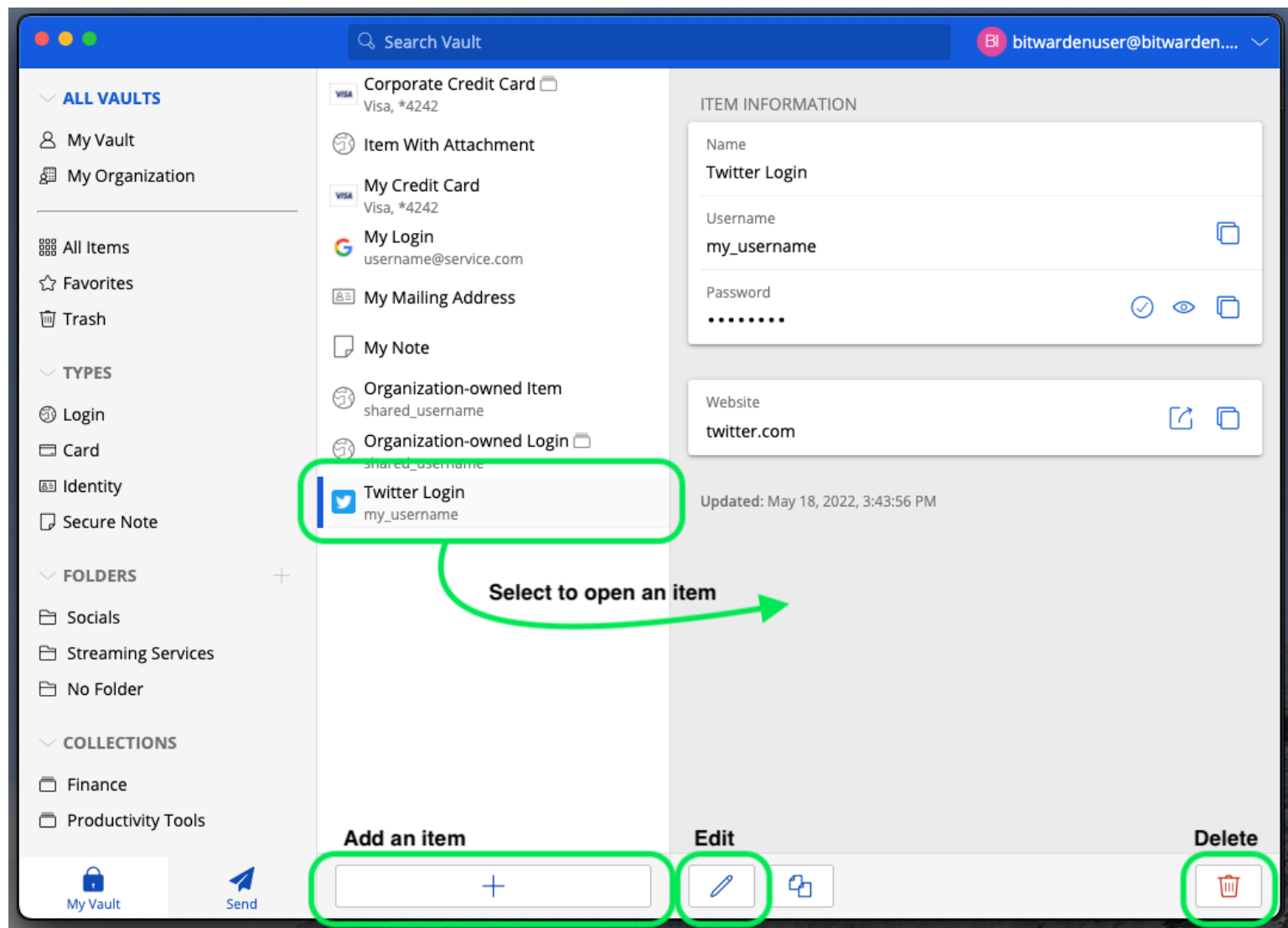
Manage an item on mobile

⇒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:
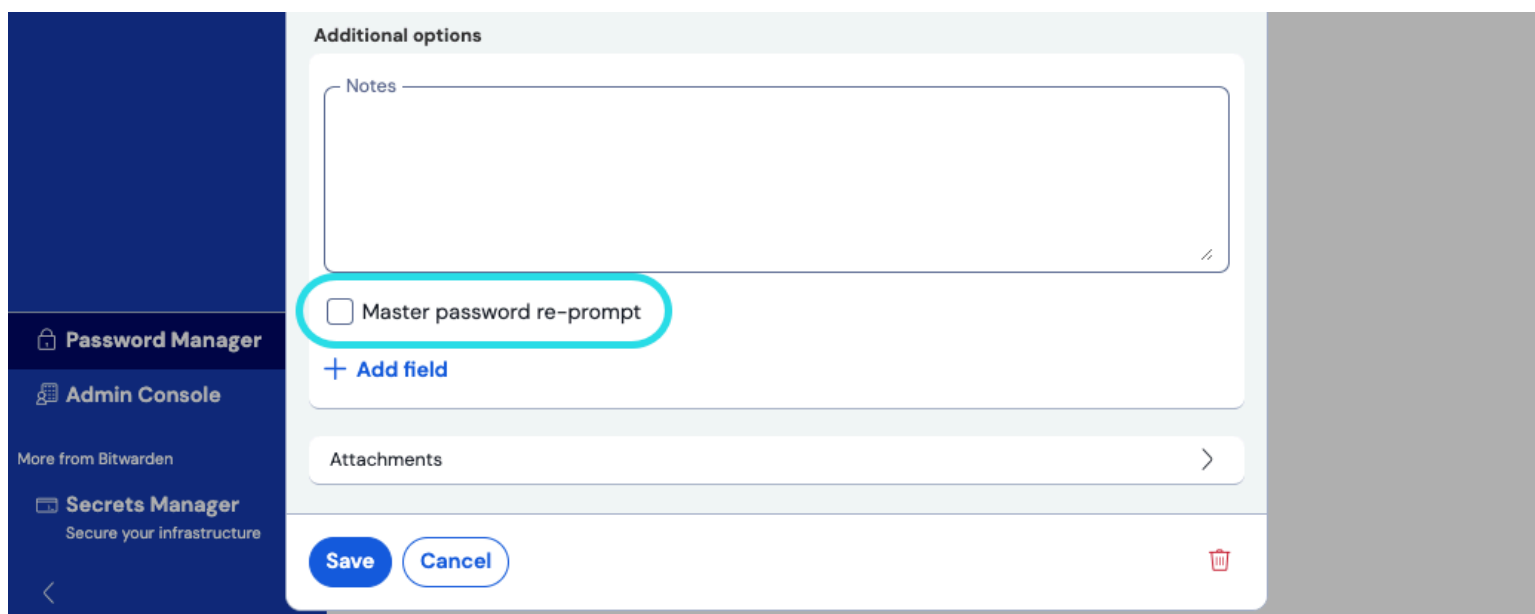

Assign to collections

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:

Trash

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