



NETWORKS**PLUS**

Keeper Security End-User Guides

Table of Contents

About Our Security 3

Browser Plugin Installation Guides 3

Mobile App Guides 3

Your Keeper Vault 4

Create Your Keeper Account 5

Account Recovery 5

Set Your Master Password 6

Create a Record 7

Organize Your Records 8

Right-Click Context Menu 9

Delete a Record or Folder 9

 Delete Multiple Records or Folders Simultaneously 10

Favorites 10

Sharing Records and Folders 11

 Share a Record 11

 Sharing Permissions 13

 Share a Folder 14

Key Features 15

 Password Generator 15

 Passphrase Generator 16

 Quick Search and Recently Viewed 17

 Launch 17

 Security Audit 18

 Record History 20

Changing Passwords with KeeperFill 21

Set Up Multi-Factor Authentication 22

 Device Approval Options 22

 Device Approval Request 23

 Two-Factor Authentication 23

 2FA for Your Keeper Vault 23

 Text Message Setup 24

 Authenticator App (TOTP) Setup: 26

About Our Security

Keeper is a Zero-Knowledge platform. The data stored in a Keeper vault is encrypted and decrypted locally on the user's device.

How Keeper protects your information:

Keeper Security employees have no ability to decrypt customer data, because the encryption keys are managed by the customer. In addition to zero knowledge architecture, Keeper supports a number of two-factor authentication methods including Google Authenticator, Microsoft Authenticator and SMS.

Browser Plugin Installation Guides

- [KeeperFill for Chrome](#)
- [KeeperFill for Firefox](#)
- [KeeperFill for Edge](#)

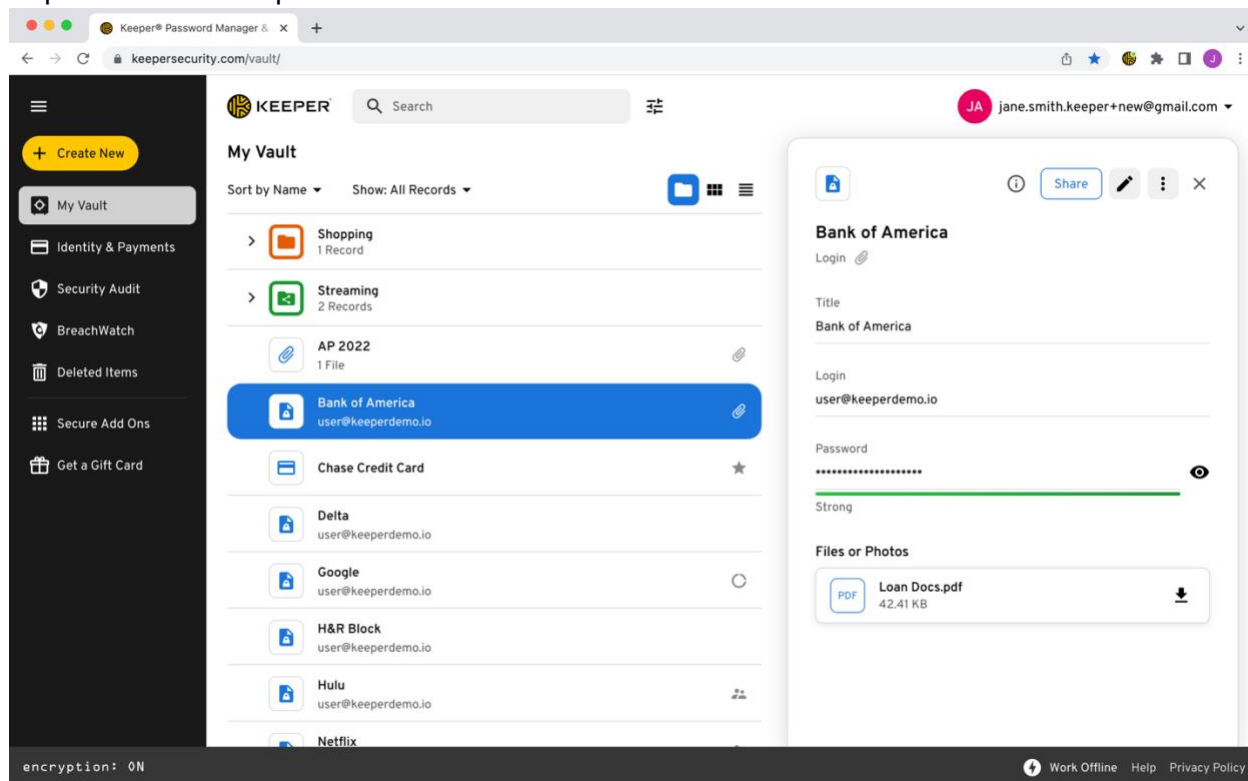
Mobile App Guides

- [Apple iOS Phones and Tablets](#)
- [Android Phones and Tablets](#)

[CLICK HERE TO ACCESS KEEPER'S YOUTUBE CHANNEL FOR INSTRUCTIONAL VIDEOS](#)

Your Keeper Vault

With Keeper, your passwords, logins and other personal information are saved in a private, digital vault. It is here where you can view and edit all your website login credentials and details, as well as store important files and photos.



Keeper Vault

If you've already loaded Keeper on your mobile devices, you can simply login to the Web Vault with your email address, Master Password and Two-Factor Authentication (if enabled on your account).

Login to the Keeper Web Vault:

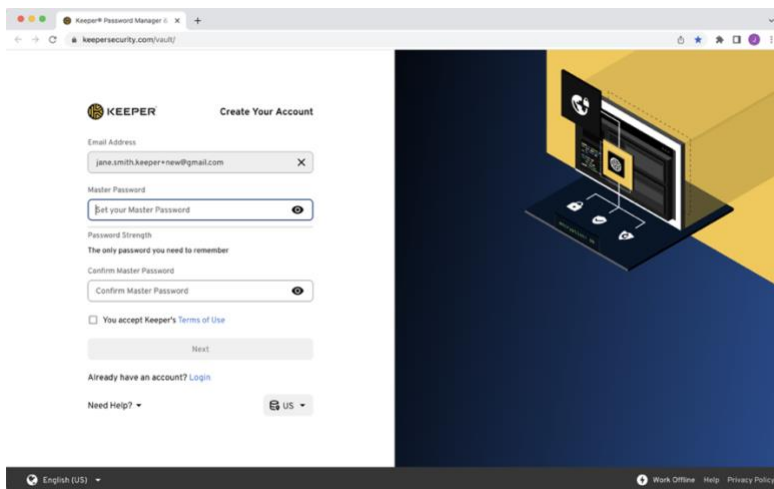
- <https://keepersecurity.com/vault> (United States)

Create Your Keeper Account

To create your Keeper account, first enter your email address then you will be asked to create and confirm a **Master Password** which will be the only password you have to remember.

We recommend that you choose a strong Master Password that is only used for Keeper -- don't forget your Master Password! Administrators are not able to reset master passwords for security reasons.

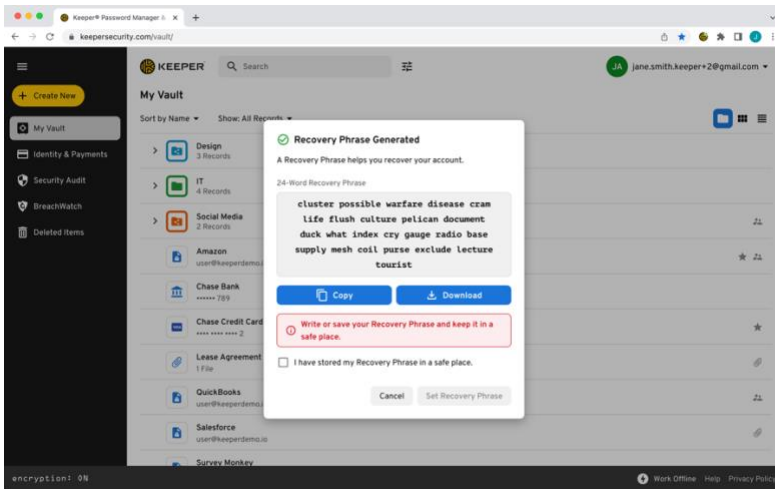
To finalize your account and proceed to your vault, you will be asked to enter the security **verification code** that was sent to your email.



Account Recovery

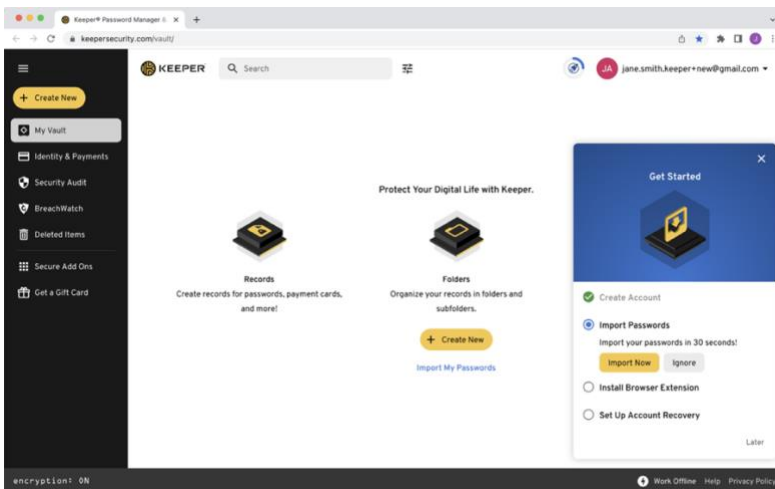
When you log into your vault for a second time, you'll be prompted to set up a 24-hour recovery phrase. If you forget your Master Password, this feature will help you quickly regain access.

Once your recovery phrase has been generated, be sure to store it in a safe place. For added convenience, you will be given the option to copy or download it.



Set Your Master Password

Upon logging in, you will be prompted to follow our Get Started wizard and install the [KeeperFill Browser Extension](#).

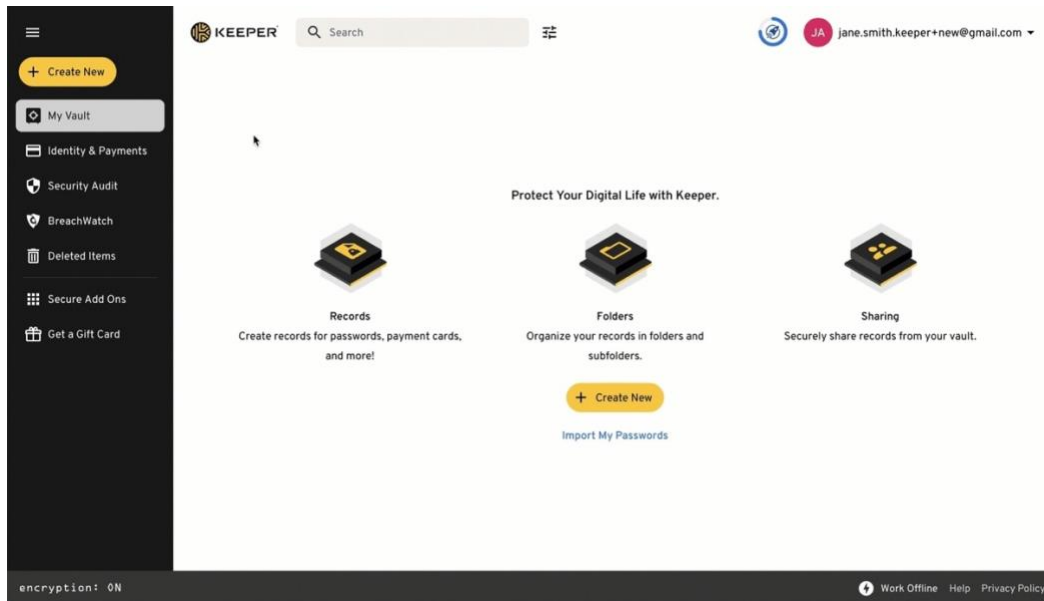


Create a Record

Your passwords, logins, credit card numbers, bank accounts and other personal information are saved in your private digital Vault (as "Records") and are encrypted on your device using 256-bit AES.

Click + to Create New > Record.

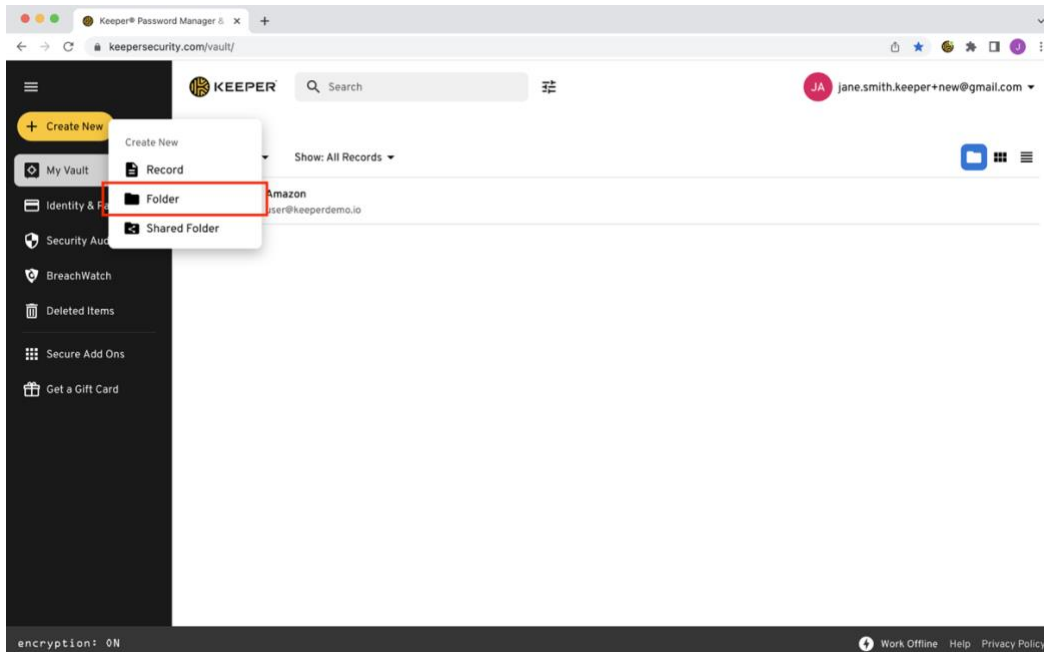
- Choose a [Record Type](#) from the dropdown menu ("Login" is the default type)
- Enter a name for the Record and click **Next**
- Enter the Login (Username or Email)
- Enter the Password or click the **dice icon** to generate one (more on that [here](#))
- Enter the Website Address
- Enter Notes, add [Files & Photos](#), a [Two-Factor Code](#) and [Custom Fields](#)
- Click **Save** to finish



Create a Record

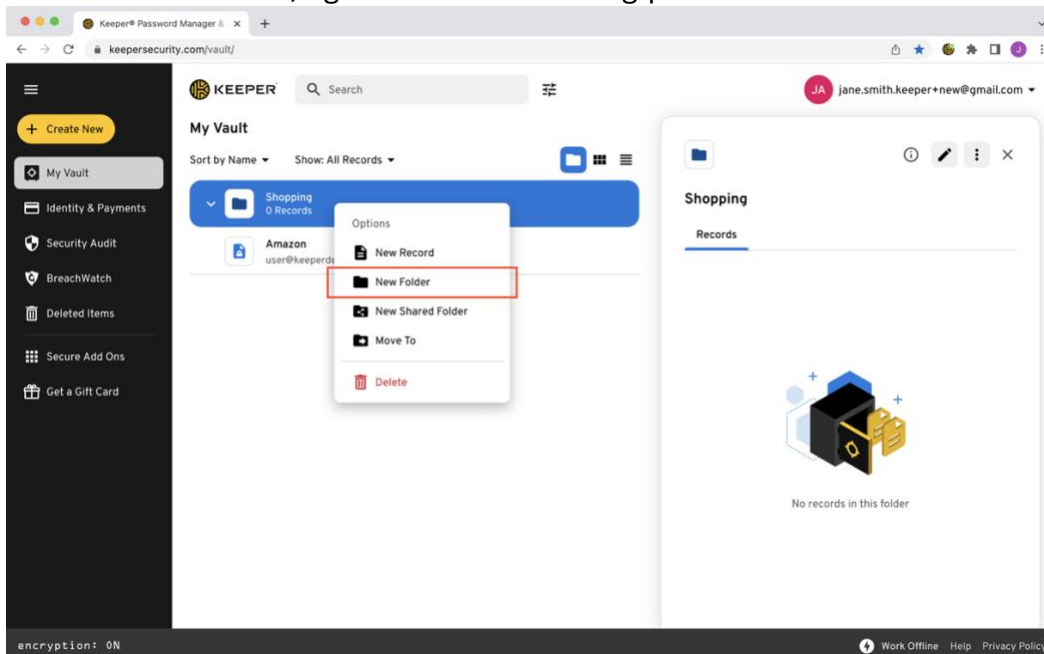
Organize Your Records

With Keeper you can organize your records into folders and subfolders. To create a folder, click on **+ Create New > Folder**. Enter the name of the folder and click **Create**.



Create a Folder

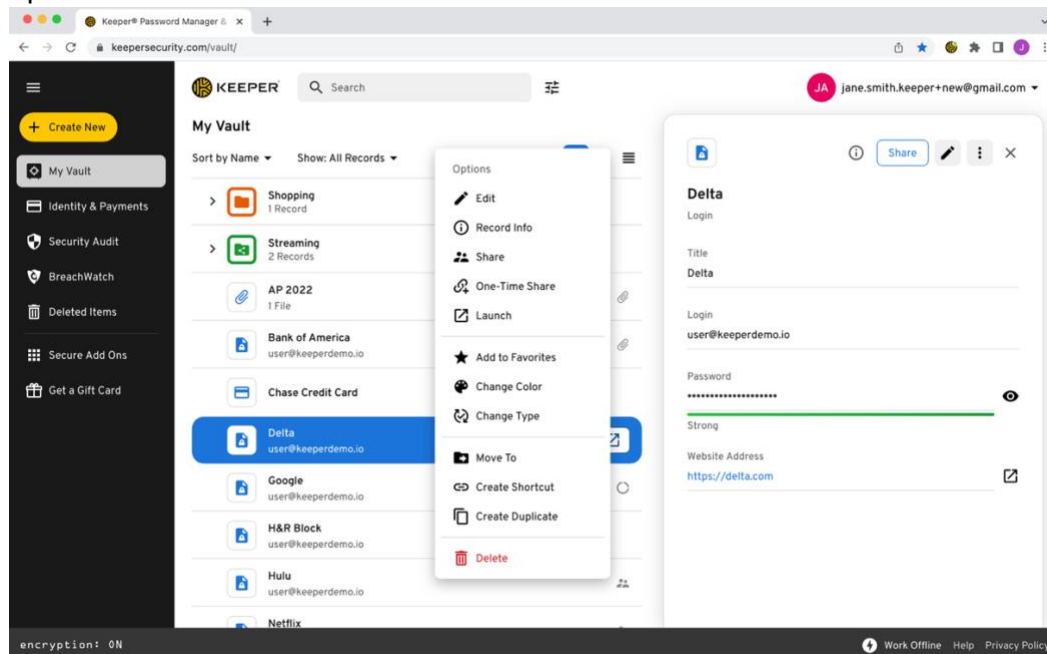
To create a subfolder, right-click on an existing/parent folder and select **New Folder**.



Create a Subfolder

Right-Click Context Menu

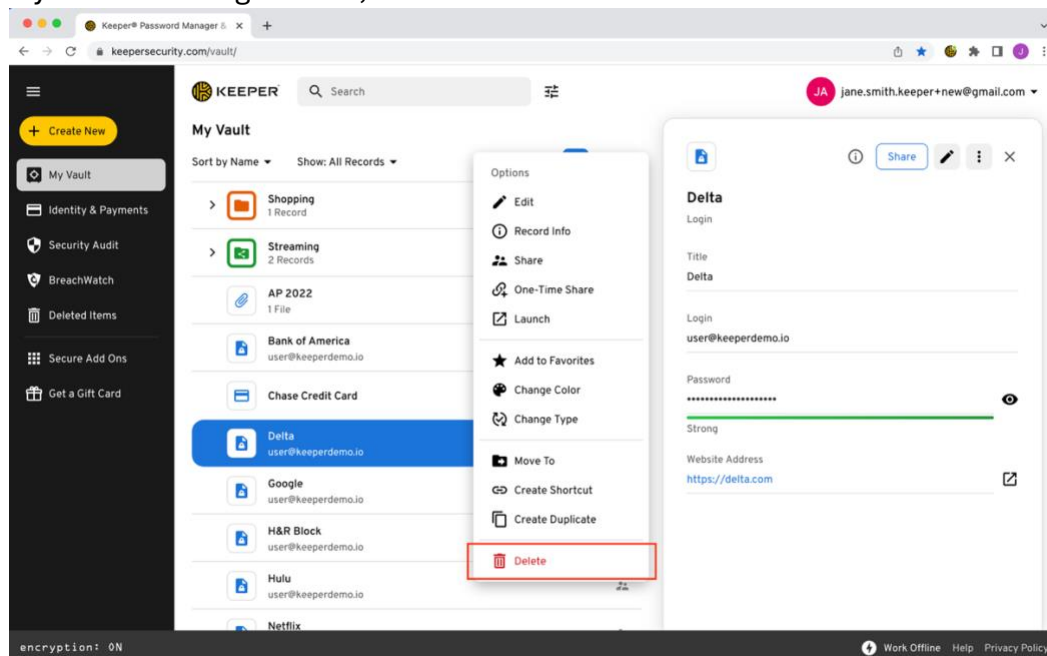
You can perform a number of actions by right-clicking on a record or folder to generate a contextual options menu.



Right-Click Context Menu

Delete a Record or Folder

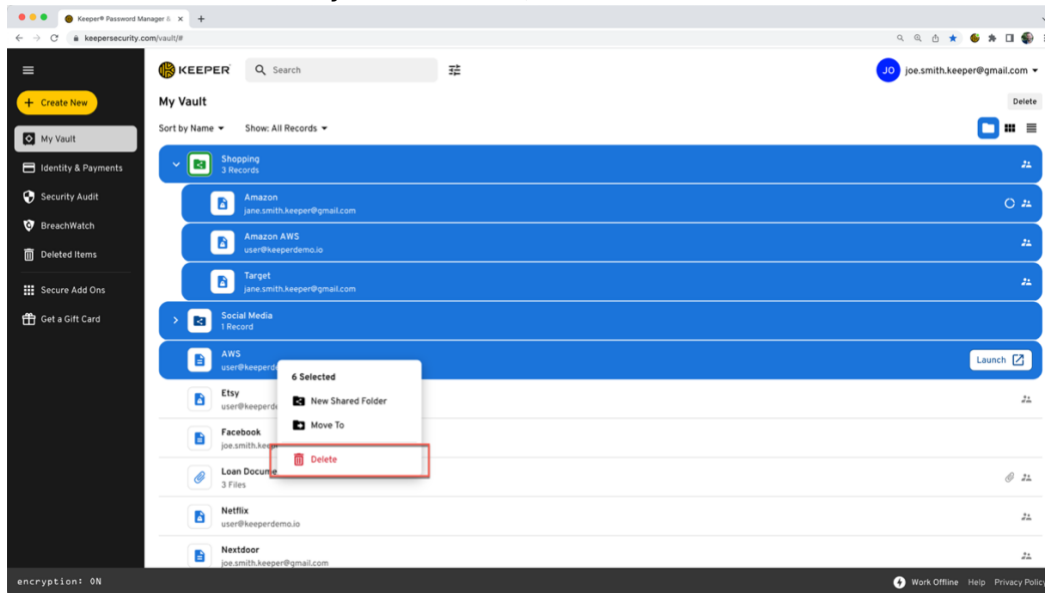
Right-click on a record or folder and select **Delete**. Click **OK** to confirm. If you are deleting a folder, all records in the folder will also be deleted.



Delete a Record

Delete Multiple Records or Folders Simultaneously

Ctrl/Cmd-click multiple records or folders to select for deletion. Right-click on the selection and select **Delete**. Click **OK** to confirm. Shift-click for selecting a list of items is also supported. If a folder is included in your selection, all records in the selected folder will be deleted.

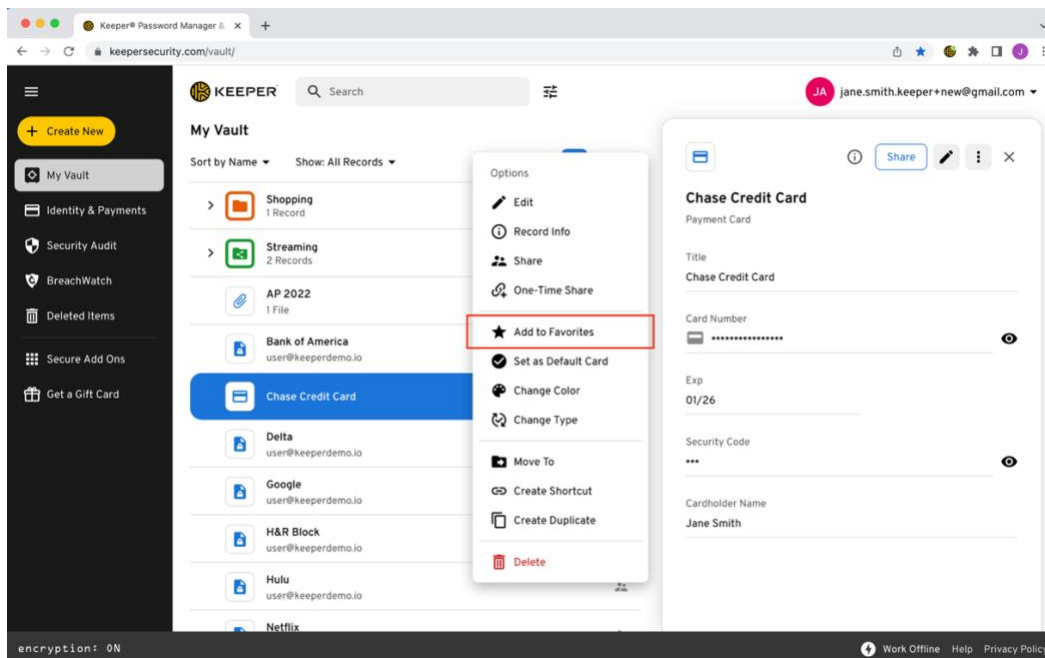


Delete a Record

Deleted records can be found in the "Deleted Items" section of your vault (for paid consumer accounts). More information on Deleted Items can be [found in this section](#).

Favorites

Record Favorites are used to easily identify your most frequently used records. Right-click on a record and select **Add to Favorites**.



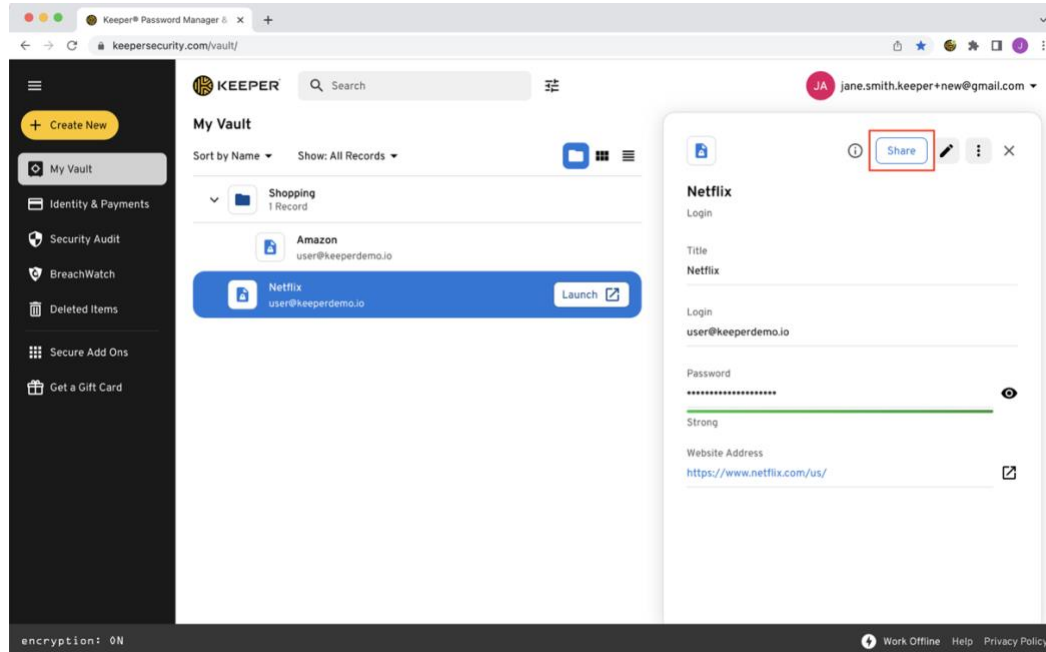
Add a Record to Your Favorites

Sharing Records and Folders

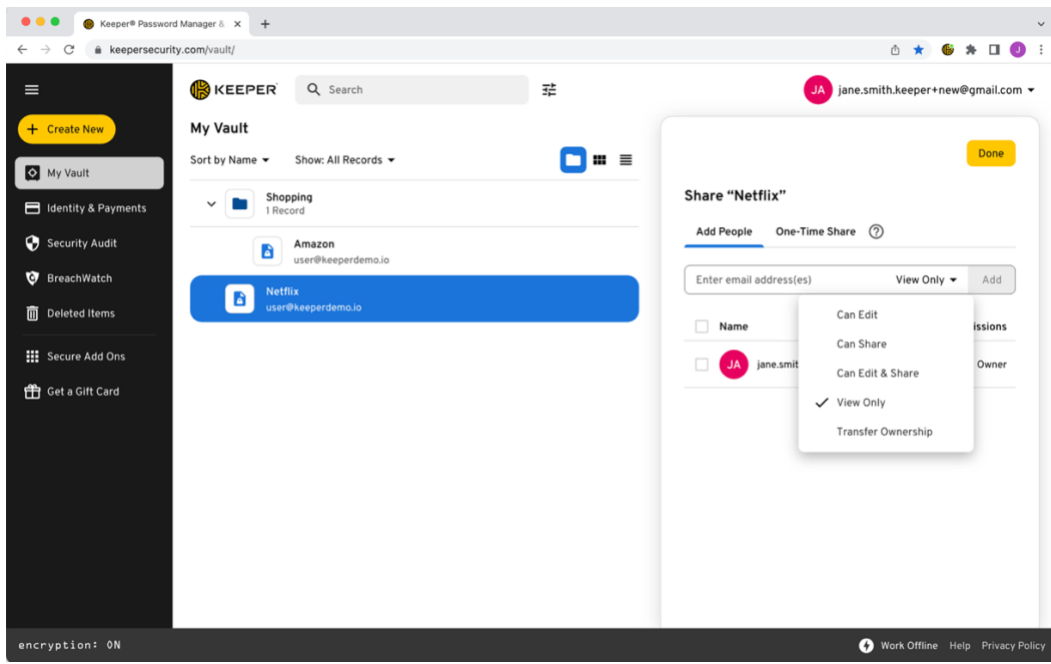
Securely share records and folders with other Keeper users such as family, friends and colleagues. If you attempt to share a record or folder with someone who is not an existing Keeper user, they first receive an email inviting them to sign-up for Keeper.

Share a Record

While viewing a record, click **Share**.



Enter the email(s) of the user(s) you would like to share with, then choose their permission type from the dropdown menu.



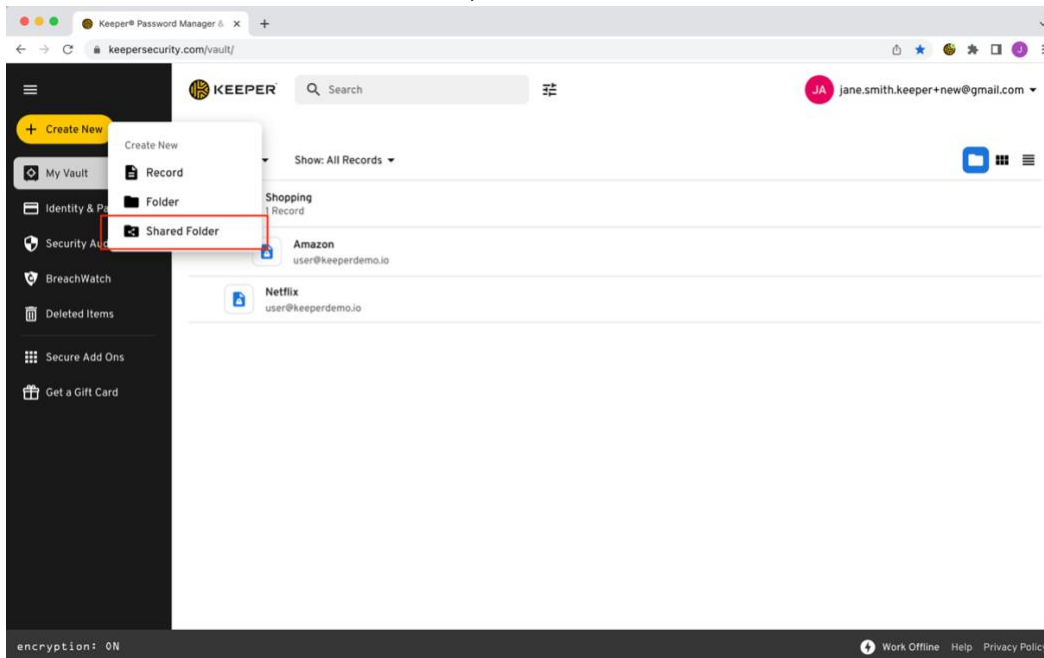
Sharing Permissions

Permission Name	Permission Level
Can Edit	User can edit this record
Can Share	User can share this record
Can Edit & Share	User can edit and share this record
View Only	User can only view the record
Transfer Ownership	User will obtain ownership the record and control the sharing permissions

Keeper "One-Time Share" provides time-limited secure sharing of a record to anyone without having to create a Keeper account. To learn more about One-Time Share, click [here](#).

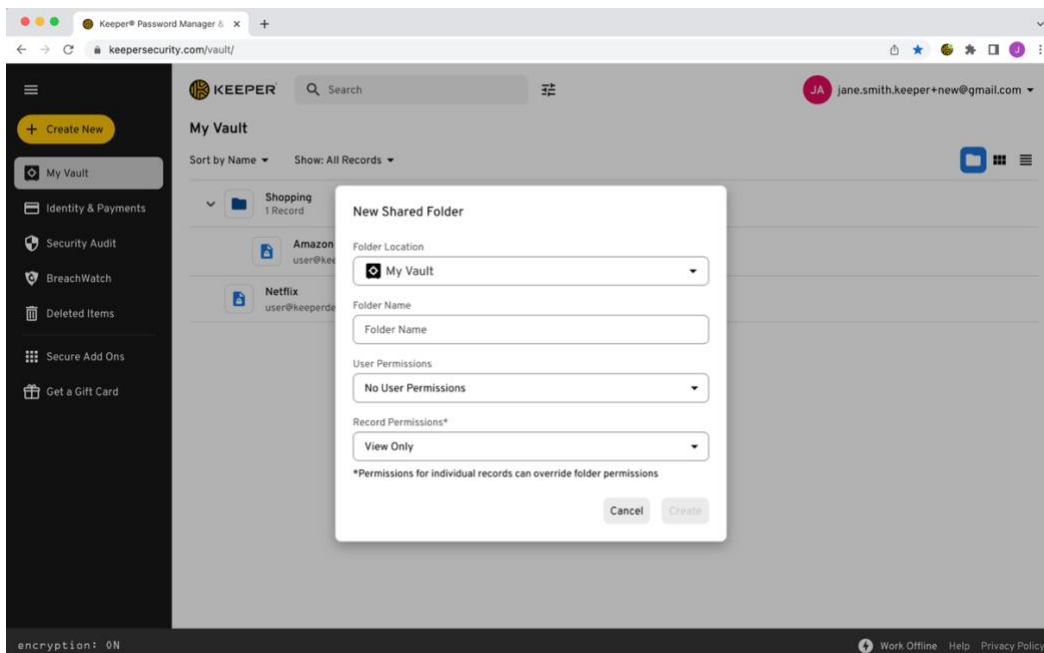
Share a Folder

Shared folders allow you to share multiple records at once and new records can be added to the folder as needed. To create a Shared Folder, click **Create New > Shared Folder**.



Create New > Shared Folder

Choose where you would like to nest the folder using the dropdown menu and enter a name for the folder. Set the User and Record Permissions and click **Create**.



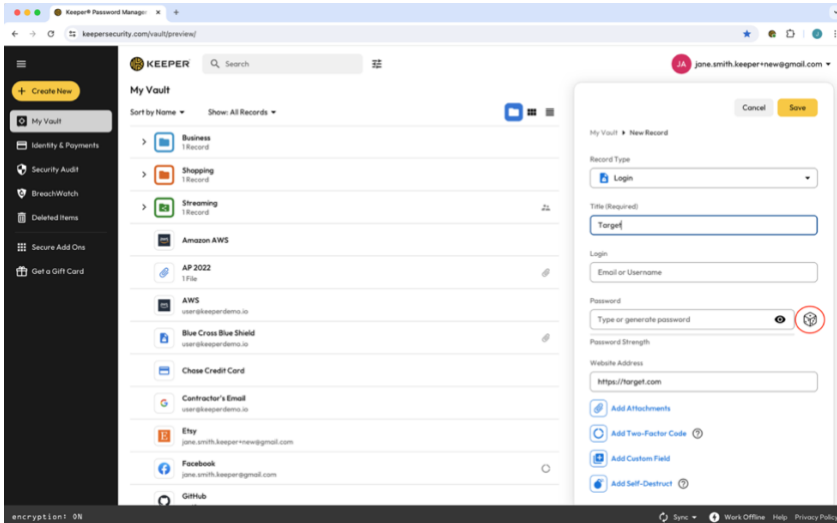
New Shared Folder Creation

Learn more about Keeper's sharing features [here](#).

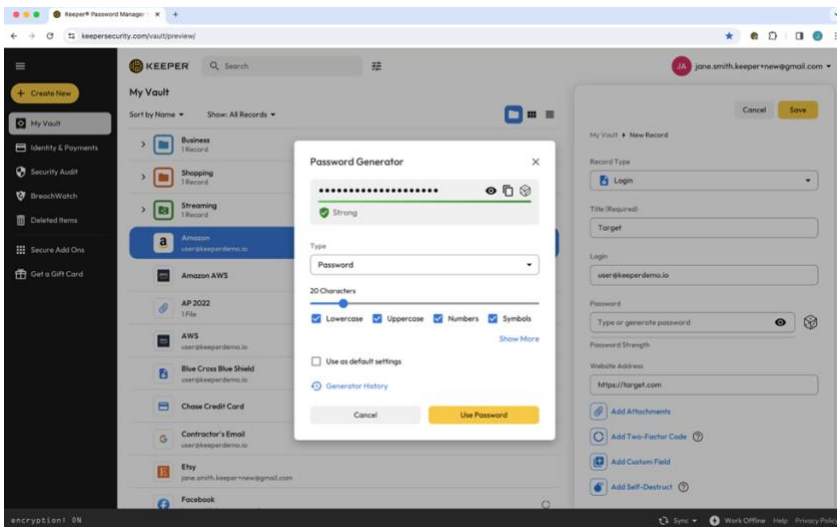
Key Features

Password Generator

Long, random passwords that are created for each login help protect your information and reduce your exposure to data breaches. Keeper generates and securely stores strong, random passwords for all of your sites and apps by clicking on the **dice icon**. The default password length for generated passwords is 20 characters. The length slider can be used to generate longer or shorter passwords for specific sites.



Password/Passphrase Generator

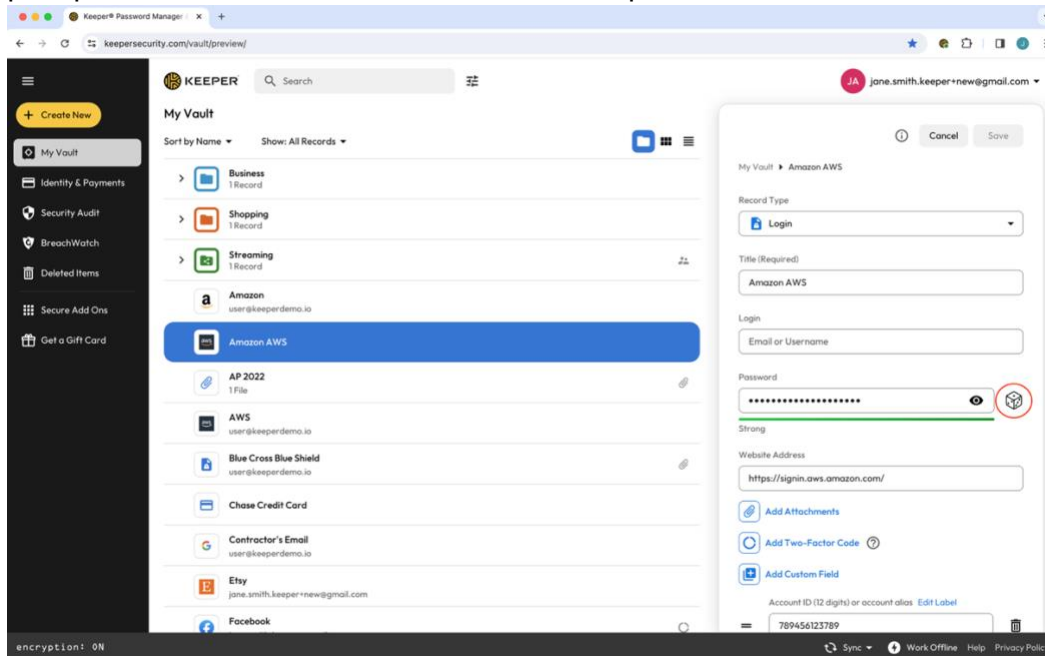


Password Customization

This will NOT automatically change the website's existing login password. You must still visit the corresponding website's "Change Password" form to update the old password to match the new, stronger password. Click [here](#) to learn how to easily change your password with KeeperFill.

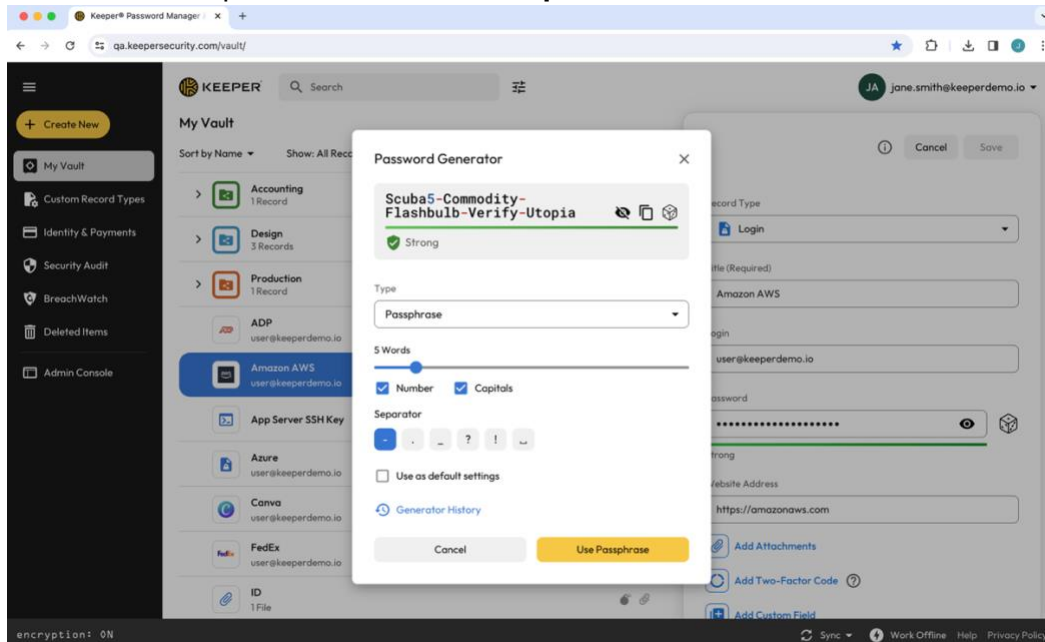
Passphrase Generator

Similar to Keeper's password generator, a click of the **dice** will generate a highly secure, random, yet easy-to-remember passphrase for any of your accounts stored in Keeper. By combining multiple words, passphrases are a more secure alternative to passwords.



Password/Passphrase Generator

Click on the dropdown and select **Passphrase**.

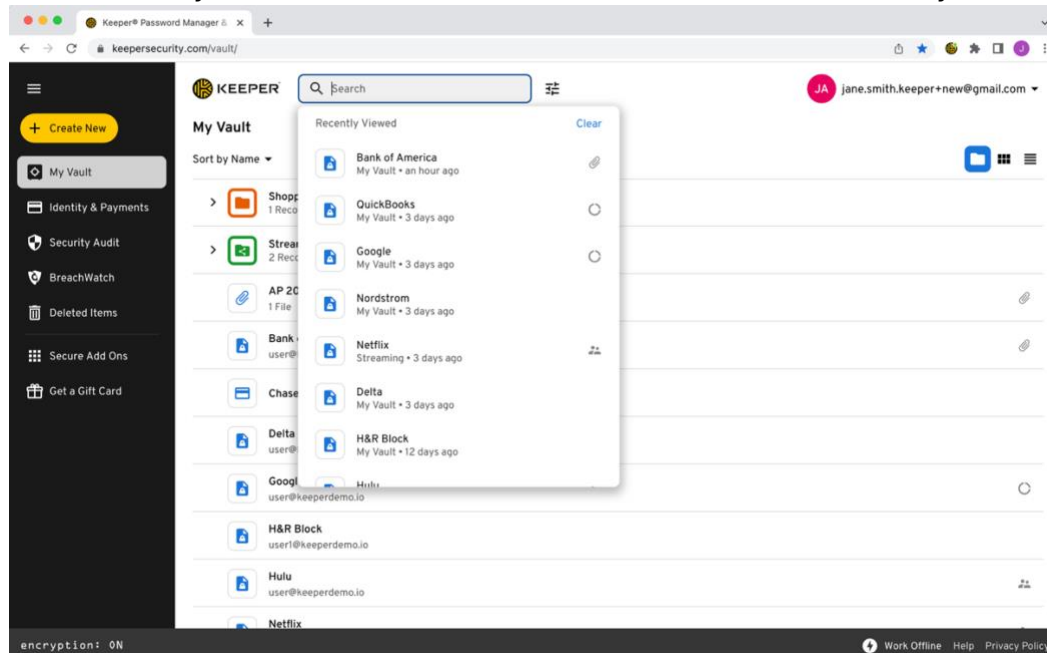


Select Passphrase

A strong passphrase includes a mix of uppercase and lowercase letters, numbers and symbols. You can use numbers, symbols or spaces to separate each word of the passphrase.

Quick Search and Recently Viewed

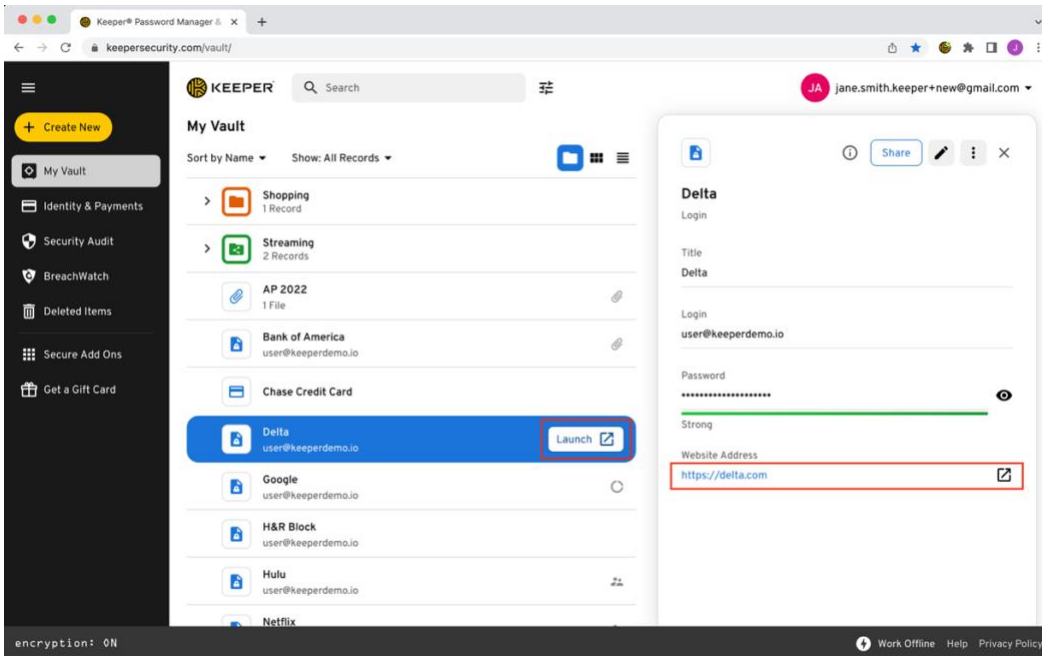
Quick search shows recently viewed items and improves sort results. Click within the "Search" field to narrow down your results based on search terms or to reveal recently viewed items.



Quick Search and Recently Viewed

Launch

Launch allows you to quickly navigate to your favorite websites. Simply click a record's **Website Address**, **Launch button**, or **launch icon** to launch the target site and login with Keeper in a new window.

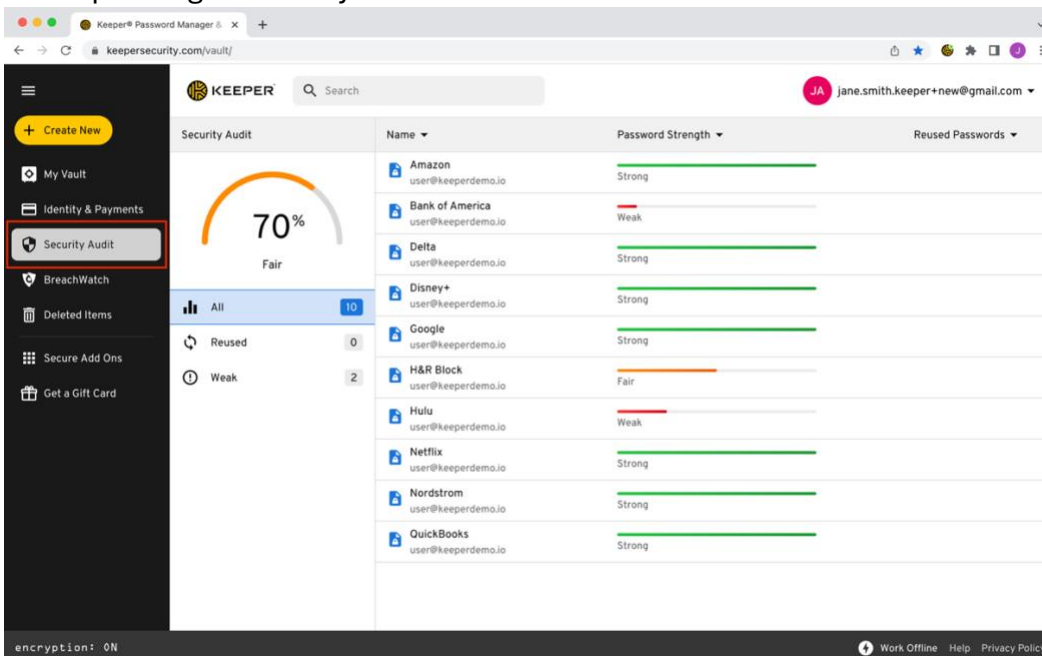


Launch

Security Audit

The Security Audit screen gives the passwords stored in your vault an overall security score based on password strength. You can clearly view information about each record's password strength and reuse from this screen.

You can easily view a record that contains a high-risk password by clicking on it from the provided list. To resolve the risk, you will be directed to change the password at the record's website and then update the corresponding record in your vault.

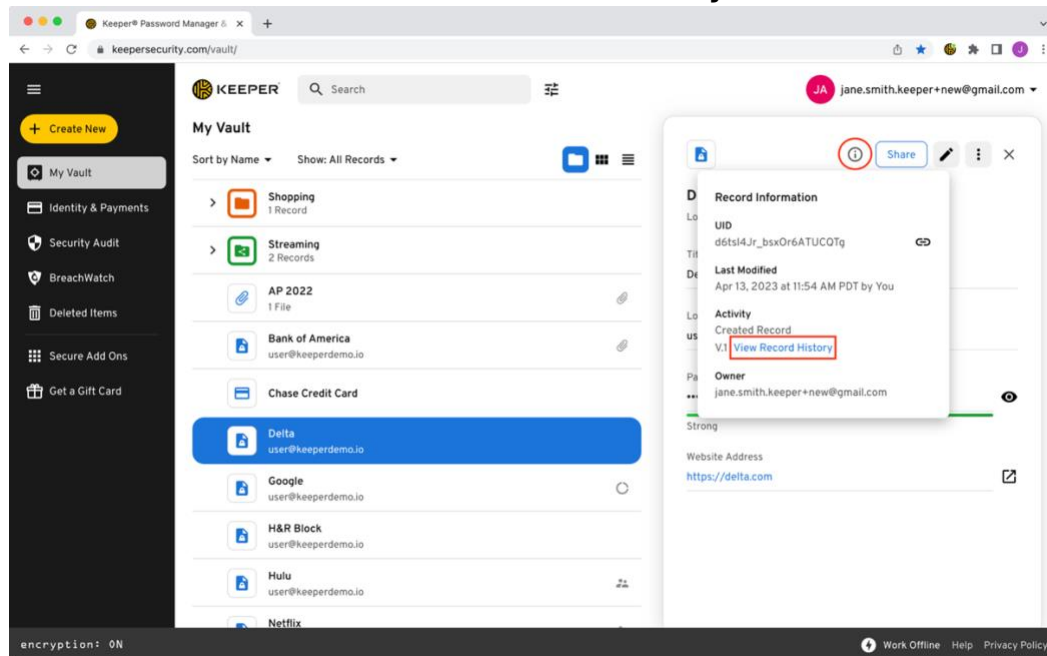


Security Audit

Learn more about Security Audit [here](#).

Record History

Keeper provides you with the ability to view and restore previous versions of a record by clicking on the record's **information icon** and **View Record History**.



Record Information

Changing Passwords with KeeperFill

KeeperFill makes it easy to change your passwords. When visiting a site's "Change Password" form, you will receive a prompt from Keeper asking if you would like help changing your password. By clicking **Yes**, Keeper will walk you through a few quick steps to change your password and simultaneously update the record in your vault. These steps will include a series of prompts detailing the following actions:

- Autofill your old/current password
- Automatically generate and autofill a new secure password
- Confirm the changes and save them to your vault

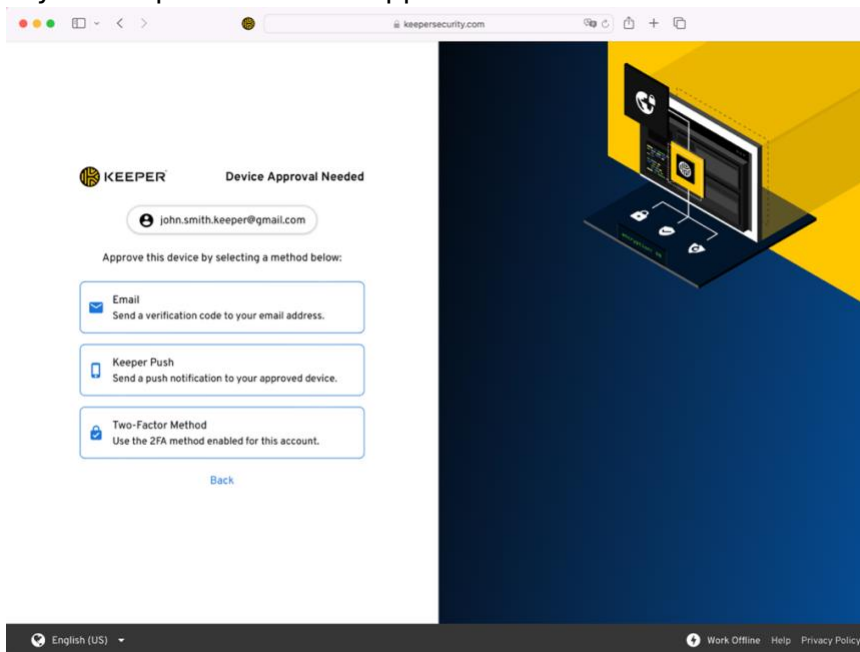
The screenshot shows a web browser window with a tab titled 'x +'. The address bar shows a URL from 'oogle.com'. The main content area displays a 'Password' change form. The form includes a heading '← Password', instructions to 'Choose a strong password and don't reuse it for other accounts.', and a 'Learn more' link. Below this, it says 'You may be signed out of your account on some devices. Learn more about where you'll stay signed in'. The form has two input fields: 'New password' and 'Confirm new password', both with icons for password strength and visibility. A 'Change password' button is at the bottom. Overlaid on the right is a KeeperFill prompt window. The prompt shows the Keeper logo, the URL 'myaccount.google.com', and the email 'Google user@keeperdemo.io'. It asks 'Would you like Keeper to help you change your password?' with 'No Thanks' and 'Yes' buttons.

KeeperFill's Prompt to Change a Password

Set Up Multi-Factor Authentication

Upon logging in, you may encounter a "Device Approval" request. If you are attempting to log in on an unrecognized device or browser, a device approval must take place before you can proceed to your Keeper Vault. Users have three methods of approval to choose from: **Email**, **Keeper Push** or **Two-Factor Method**.

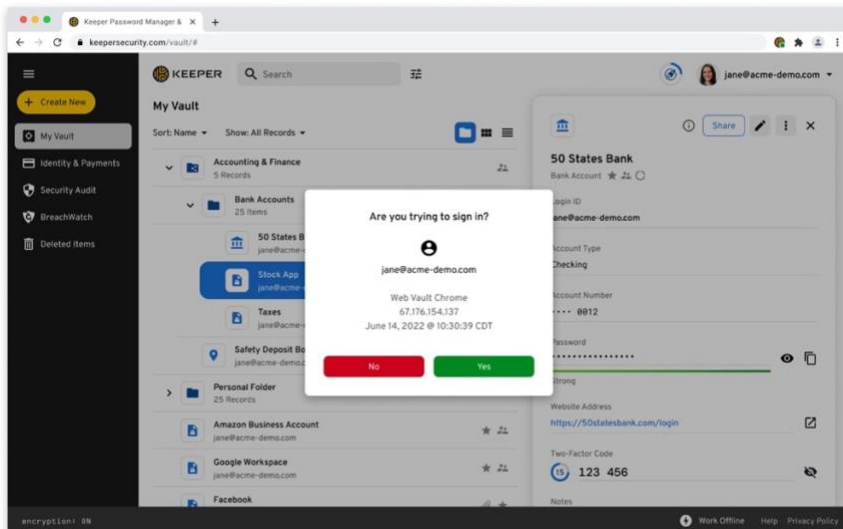
Keeper Push is Keeper's proprietary notification-based device approval system that sends a push notification to an existing, recognized device. If you select **Keeper Push**, a notification (push) will appear in your Keeper Vault on an approved device or browser.



Device Approval Options

Select **Yes** to approve the new device.

You must be actively logged into a different, recognized/approved device to receive the notification.



Device Approval Request

Once your device has been approved, you will be prompted for 2FA (if enabled), then you can enter your Master Password to proceed to your vault.

Two-Factor Authentication

Two-Factor Authentication (2FA) provides an extra layer of security when logging into your Keeper Vault or another site or application by requiring a secondary passcode upon logging in.

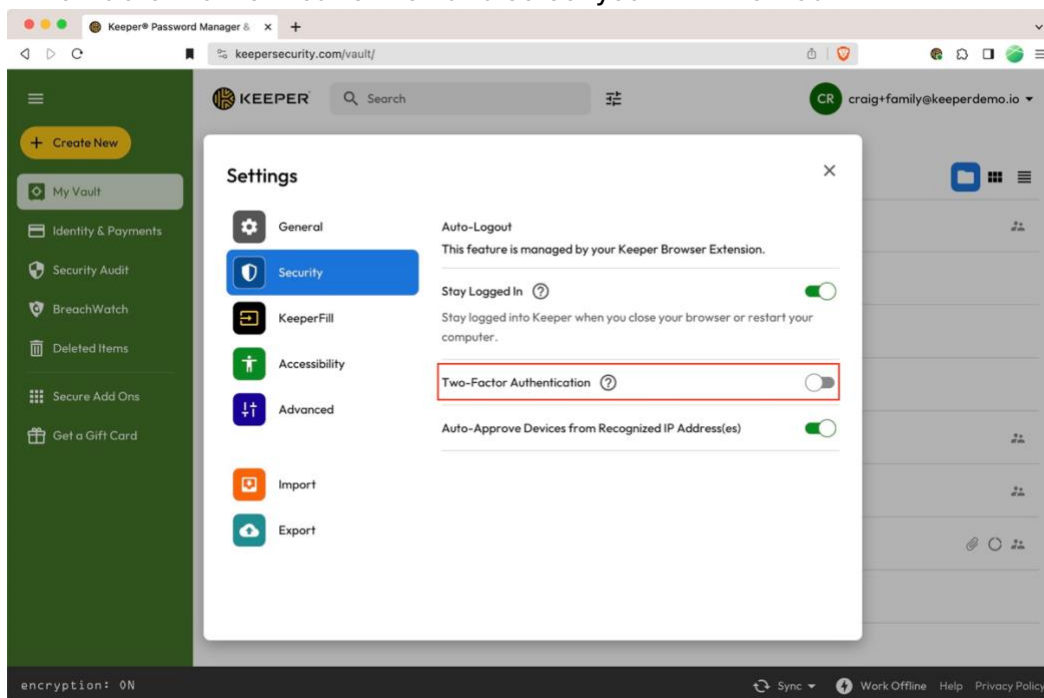
Enabling Two-Factor Authentication is advised for highly valuable or sensitive accounts (e.g. banking, medical and social media accounts).

Keeper provides two ways to take advantage of 2FA:

- To log into your Keeper Vault.
- To login into any site or application from your Keeper Vault by embedding a Two-Factor code into your records.

2FA for Your Keeper Vault

To enable 2FA for your Keeper vault, from the Account Dropdown Menu, click **Settings > Security**, toggle "Two-Factor Authentication" on and select your 2FA method.



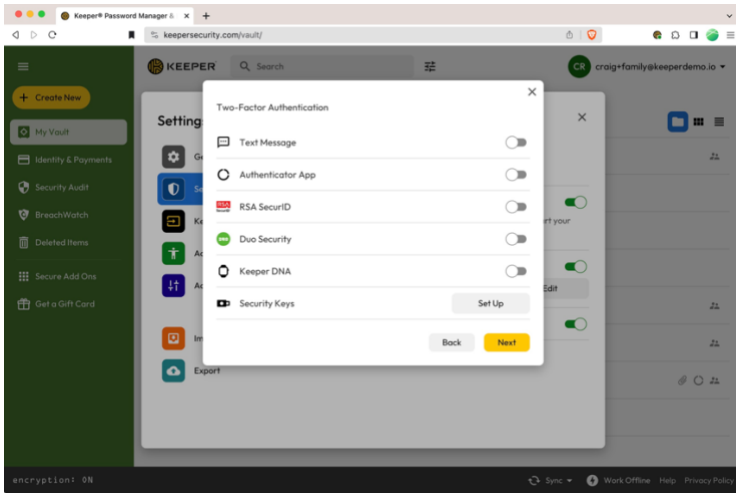
Two-Factor Authentication

Keeper supports several methods of Two-Factor Authentication:

- Text Message (SMS)
- Authenticator App (such as Google Authenticator, Microsoft Authenticator, etc)
- RSA SecurID (for Enterprise customers)

- Duo Security (for Enterprise customers)
- Keeper DNA (using Apple Watch or Android Wear devices)
- FIDO2 Security Keys (or device passkeys)

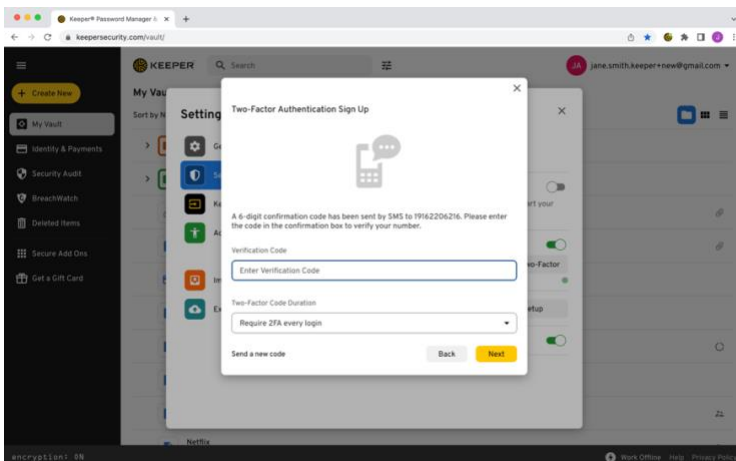
Text Message Setup



(1) The Text Message toggle is on by default. Select a **Region** from the dropdown (US+1 by default), enter your **10-digit phone number including your area code** and click **Next**.

(2) To verify that you trust this number and device, **enter the Keeper web code** that was sent to the phone number you provided. Select your 2FA code duration from the dropdown menu and click **Next**. Codes will only last for a minute; if you need another code sent, click **Send a new code**.

You will be prompted for 2FA every time you login to your Vault unless you select an alternative code duration. Business customers may be required to enter the code every login as determined by their Keeper Administrator.



Enter Verification Code

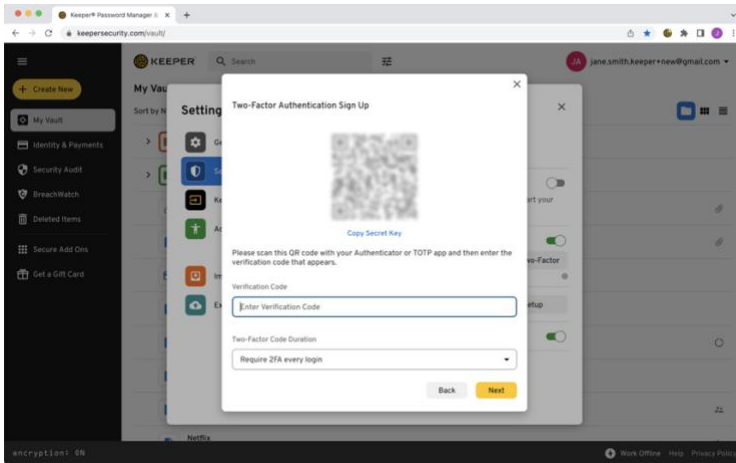
(3) Backup codes will be shown next. If you are unable to receive Two-Factor codes via the phone number you entered, you can enter one of the codes listed instead. Click **I have written these codes down** to finish.

If you are NOT receiving SMS messages from Keeper, please use the TOTP method.

Authenticator App (TOTP) Setup:

(1) Toggle "**Authenticator App**" on and click **Next**.

(2) Using the device that runs the the TOTP application, **scan the QR code** provided or manually enter the secret key. The app will then acknowledge the QR code and produce a verification code.



Two-Factor Authentication Sign Up

(3) **Enter that verification code** and click **Next**.

You will be prompted for 2FA every time you login to your Vault unless you select an alternative code duration. Business customers may be required to enter the code every login as determined by their Keeper Administrator.

(4) Backup codes will be shown next. If you are ever unable to receive Two-Factor codes, you can enter one of the codes listed instead. Click **I have written these codes down** to finish.

In order for Azure MFA (using the Microsoft Authenticator app.) to be utilized as a TOTP, the Azure administrator needs to allow the verification method "Verification code from mobile app or hardware token" when setting up MFA in Azure.