Keeper Guide

TrinWare's Guide to Keeper – Cybersecurity Starts Here

Keeper is a password management service that stores and generates strong passwords for all of your online accounts

- It is important to have unique, strong passwords across your online presence.
- A strong password is long, has both upper and lowercase letters, and uses numbers and symbols throughout.
- It can be challenging to generate and remember your own passwords, and tempting to reuse passwords to compensate.
- Keeper is quick and easy to set up and use, and protects your online presence for you.

New User **Registration**

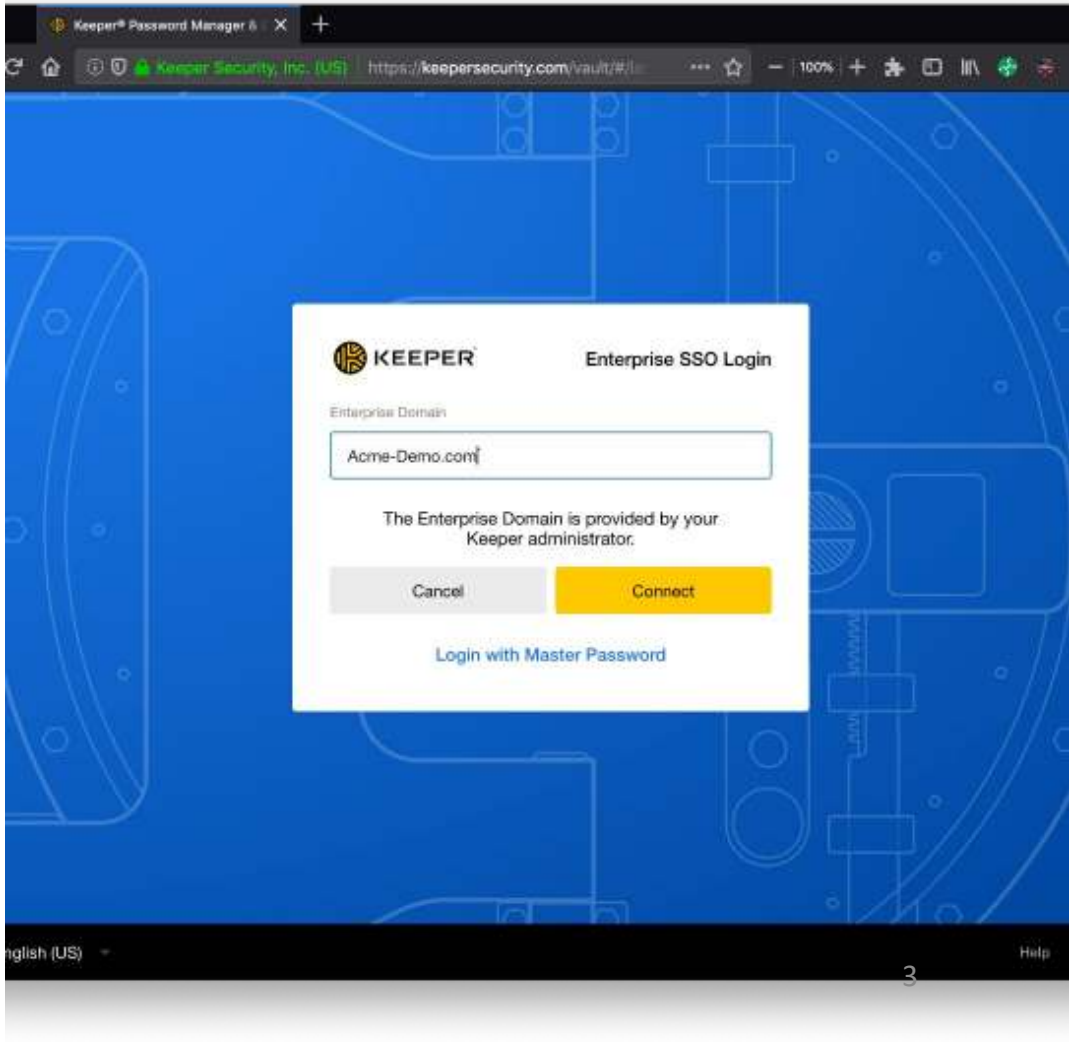
New User

First, you must choose a **Master Password**. We recommend that you select a strong Master Password that is only used for Keeper, and not used for any other service. **Do not forget your Master Password.** Enterprise customers may enforce a Master Password that adheres to company guidelines.

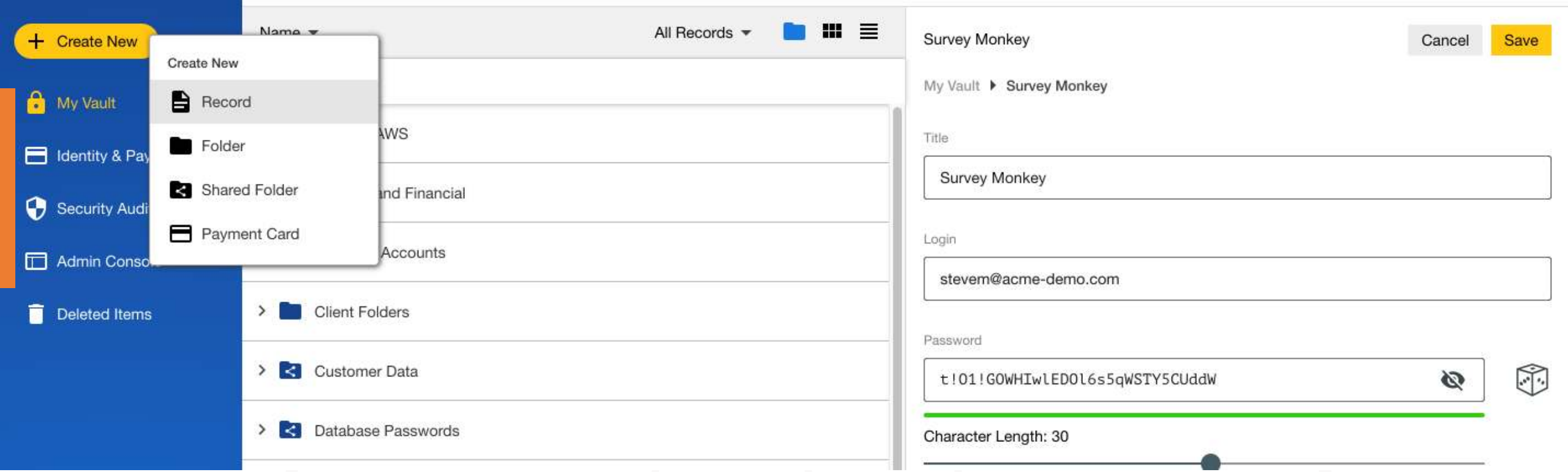
Enterprise SSO Login

Customers who login with an existing identity provider will click on **Use Enterprise SSO Login** and enter the **enterprise domain** provided by your Keeper administrator.

Enterprise users who login with SSO do not require selection of a Master Password.



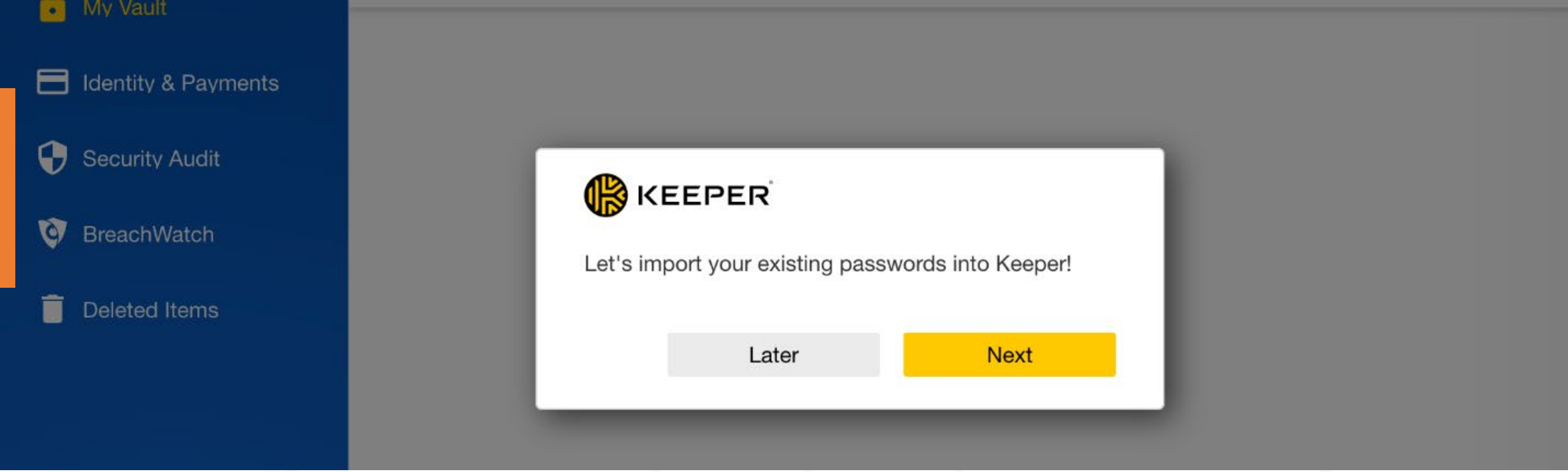
TrinWare
Hardware + Software + People



Creating **Records**

- Keeper protects you against cyber-criminals with a secure and convenient password manager. Your passwords, logins, credit card numbers, bank accounts and other personal information are saved in your private digital Vault that is encrypted on your device using 256-bit AES (Advanced Encryption Standard).
  To create a new record, from the left navigation menu, click the **+ Create New** button.

TrinWare
Hardware + Software + People



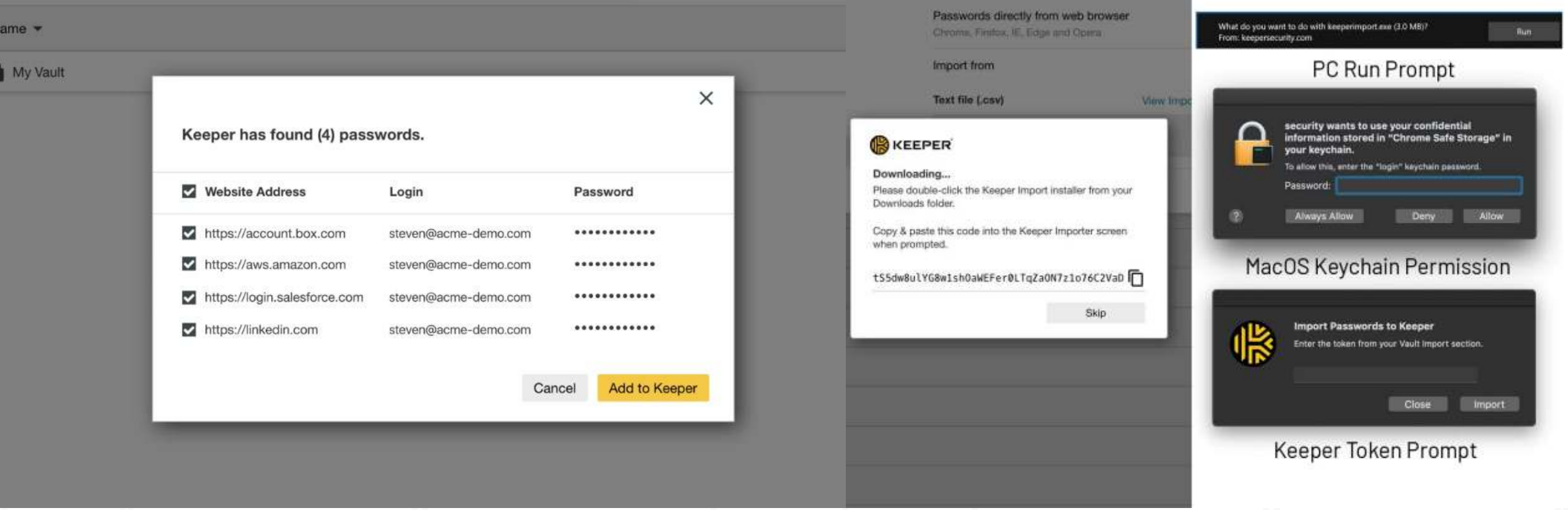
Importing **Passwords** Part. 1

- Keeper can import logins and passwords directly from your web browser, another password manager, or text file (.csv).

- To import from your web browser (Chrome, Firefox, IE, Edge, Opera) you must first install the Keeper Import Tool.

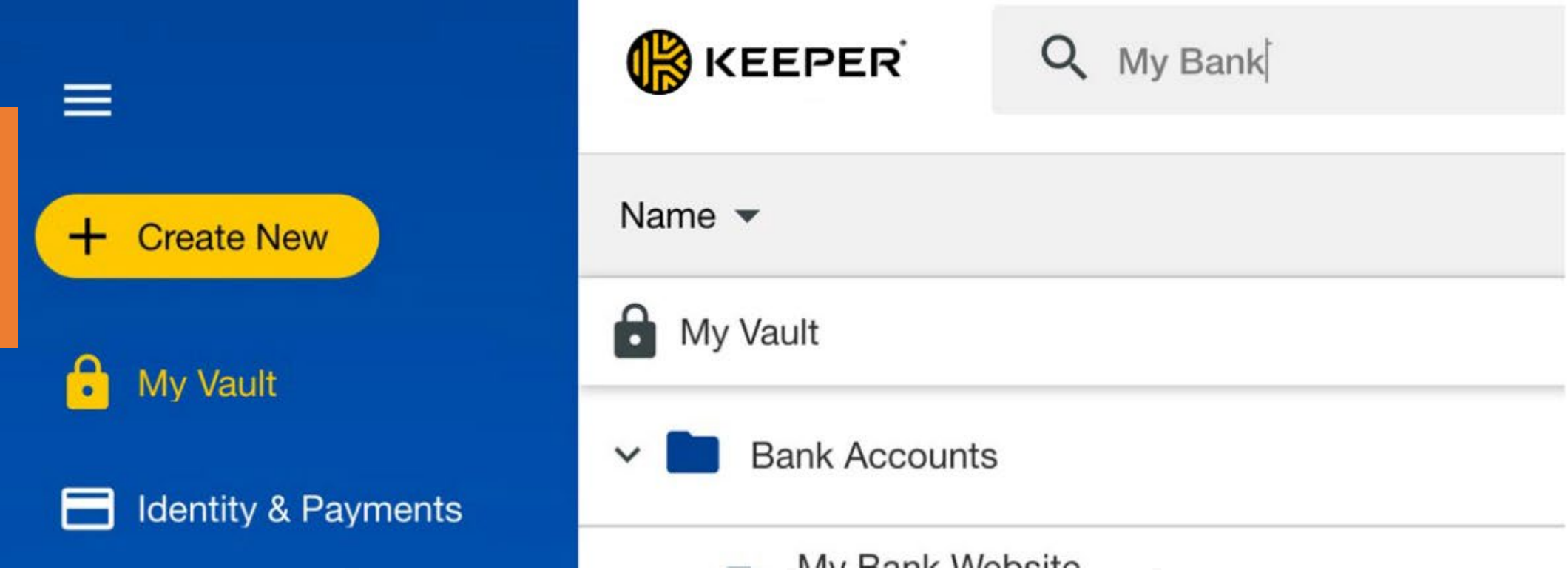
- To begin the installation, click on **Account > Settings > Import**. If you have started the import process from a mobile app and came to the web vault, the web vault will ask you to install the Keeper Import Tool. If you came fresh into the Web Vault, you can download the import tool by clicking on the **Import** button.

- Click Install to begin the download. Keeper will then walk you through the process and ask you to double click on the Keeper Import installer from your Downloads folder.



- **Copy the code** Keeper gives you. You will need this when prompted in the Keeper Importer.
- If you are using a PC, you can just click **Run** when prompted.
- If you are on a Mac, Double click the **KeeperImport.zip file** in your downloads. Then double click on the **Keeper Import App** to start the import process. You will encounter a few Keychain permission windows that will require your computer password to allow Keeper to access your web browsers.
- Keeper will then ask for your code you received from an earlier step. **Paste the code** and click **Import**.

Once the installation is complete, Keeper will report websites and their associated logins and passwords directly from your web browser. You can then scroll though and uncheck those you do not wish to import. Once you have finished reviewing the report, click **Add to Keeper** to import the selected passwords

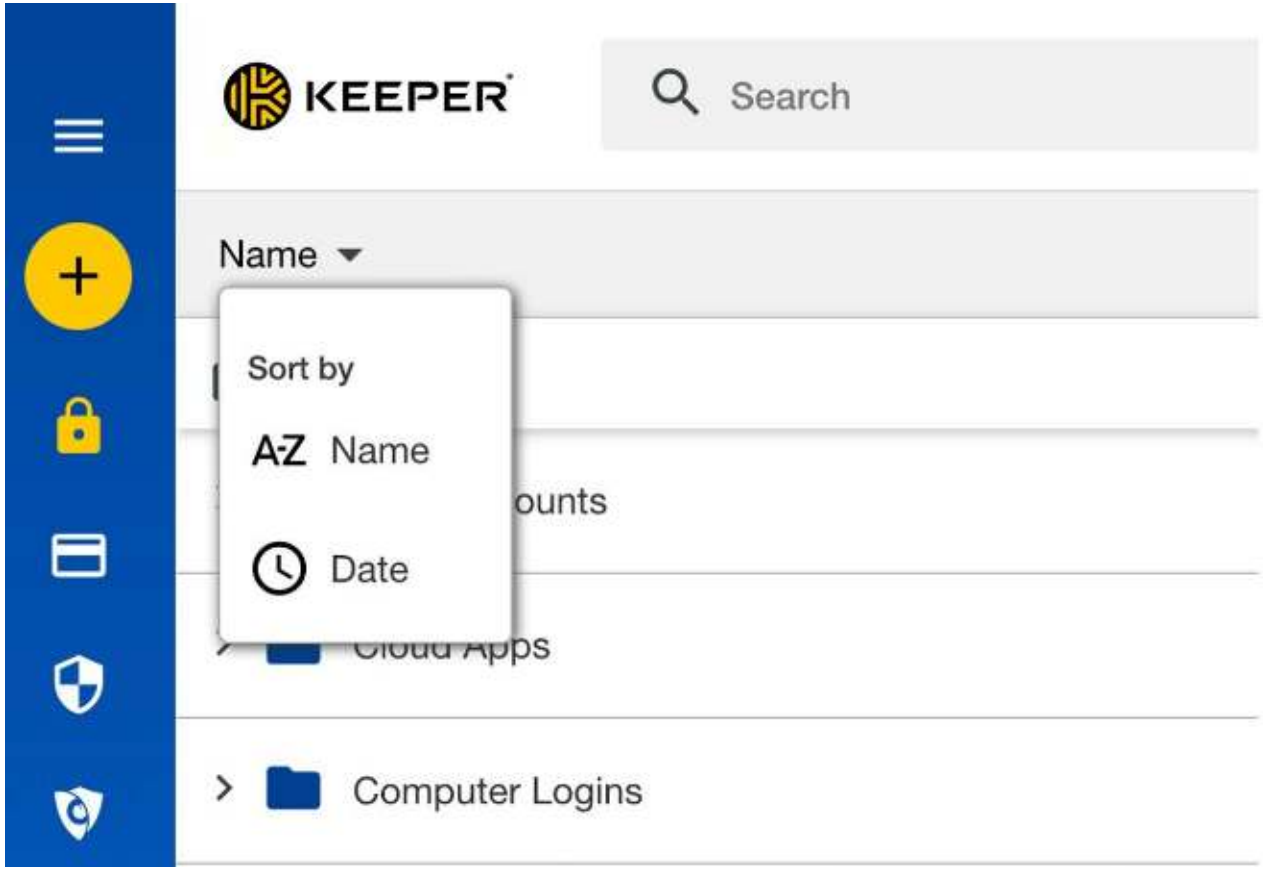


Search **Feature**

- Keeper's dynamic search feature automatically displays relevant records as you type. For your convenience, searching works in all fields within each Keeper record.

Filter **Records**

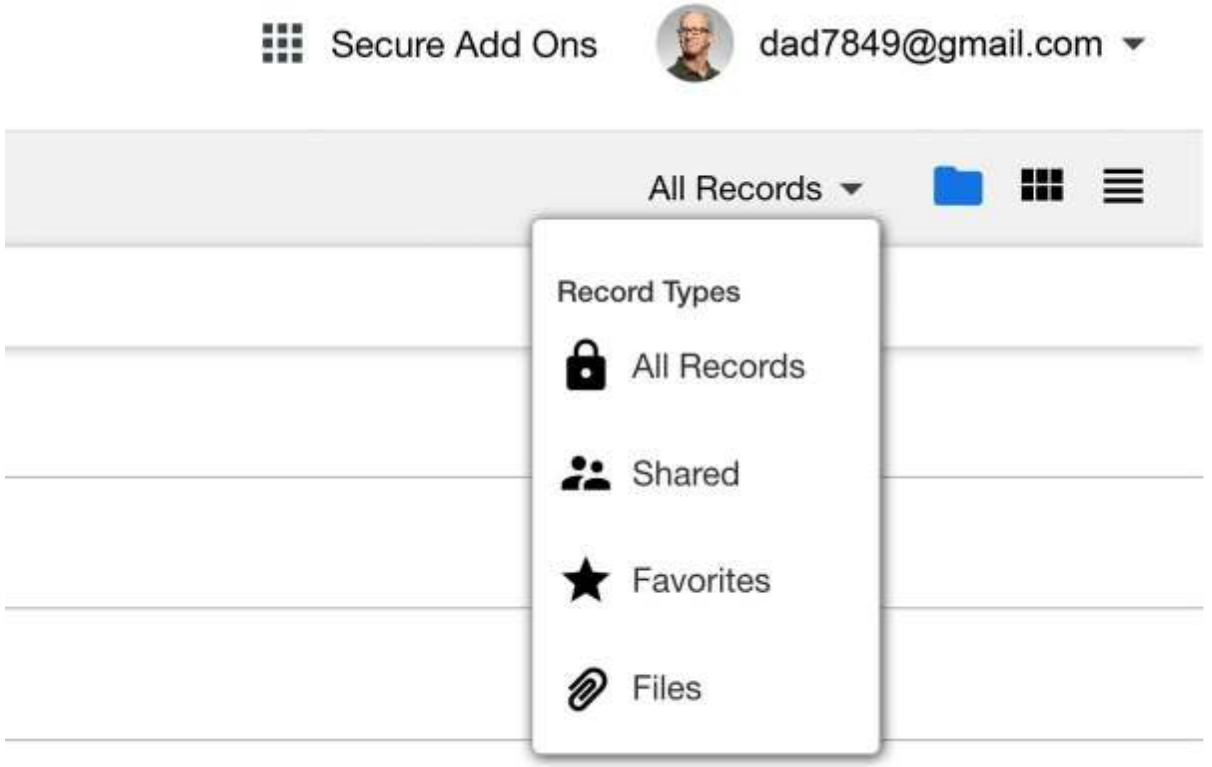
To filter by Name or Date, use the Name dropdown menu.



Deleted Records **and Record Types**

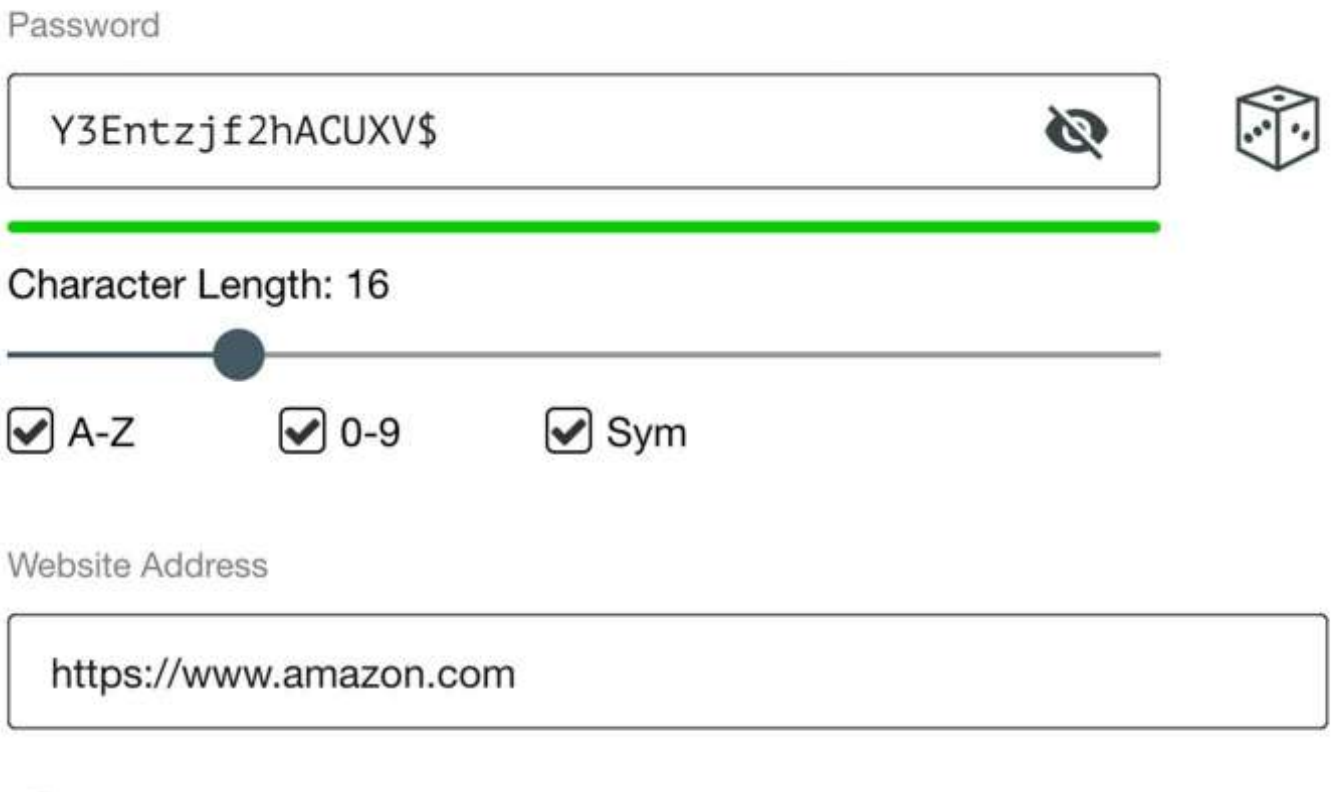
- To filter by **specific record types**, use the **All Records dropdown menu** and **buttons**.

- Deleted Records can be accessed from the left navigation menu.

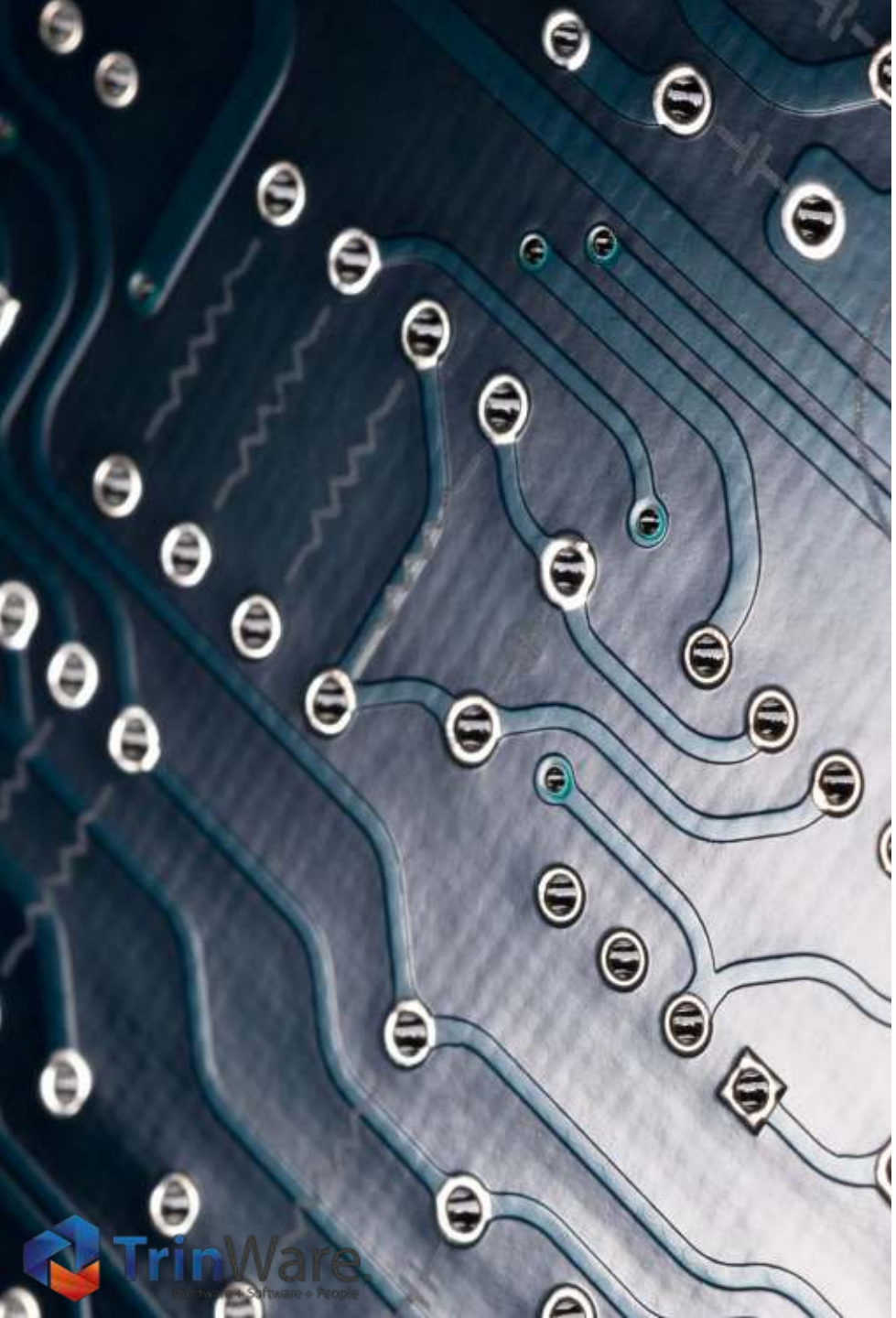


Password **Generator**

- Long, random passwords that are generated for each website help protect your information and reduce your exposure to data breaches. Keeper's Password Generator instantly creates **strong**, random passwords with a click.



TrinWare
Hardware + Software + People

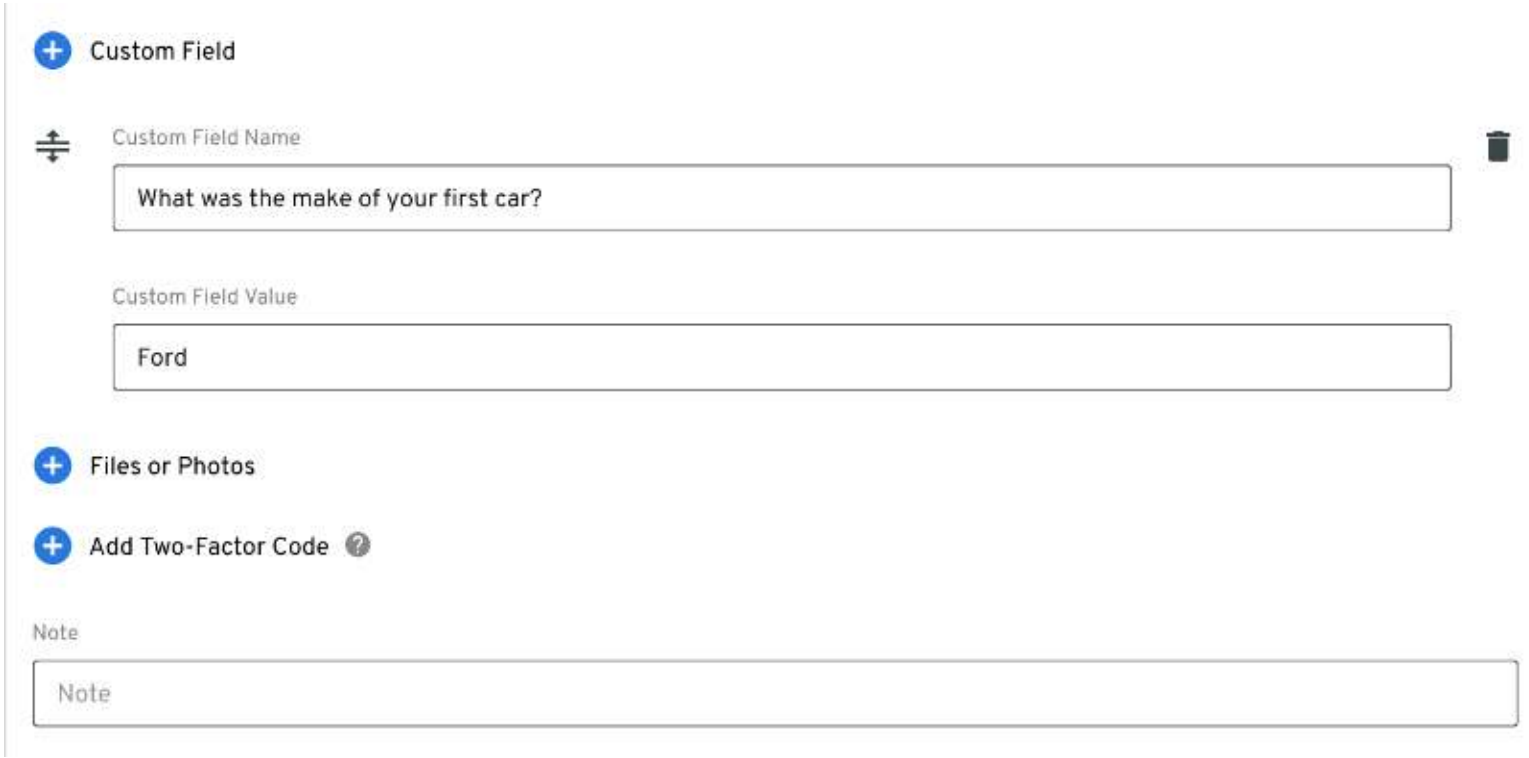


Custom **Fields** Part.1

Custom Fields can be used to store additional data such as the answer to a security question, a pin number, an account number or anything else that makes the record valuable. Custom fields are created in pairs; the "Custom Field Name" and the "Custom Field Value". The custom field value can be used to autofill fields via the KeeperFill browser extension.

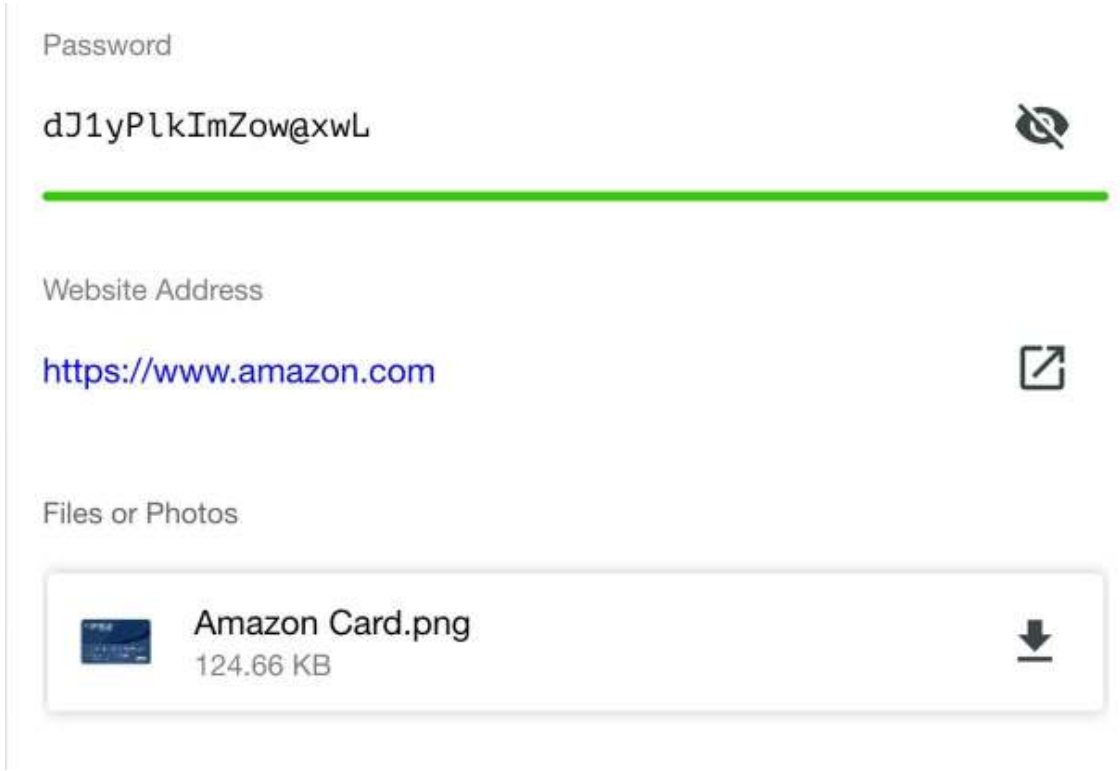
Custom **Fields** Part. 2

- To create a custom field, while viewing a Keeper record, click Edit then click on the + Custom Field heading and observe the custom field name and value appear. Custom fields can be arranged in any order by dragging them in the desired order.
- Masked custom field values are only available for Keeper Enterprise customers.
- Entering "Website Address" in the Custom Field Name and a URL to the Custom Field Value allows you to associate the username and password credential of the record to an additional website if they use the same identity.



Auto **Launch**

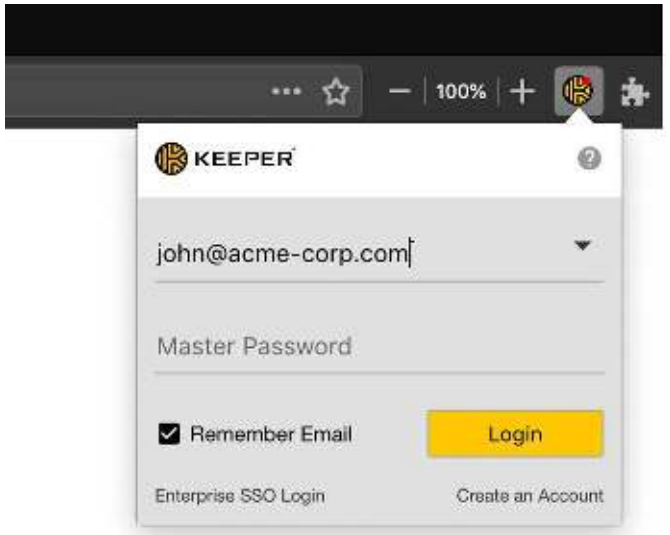
- One-click login lets you securely access your favorite websites. From your Keeper record, simply click the Website Address field and your site will launch.

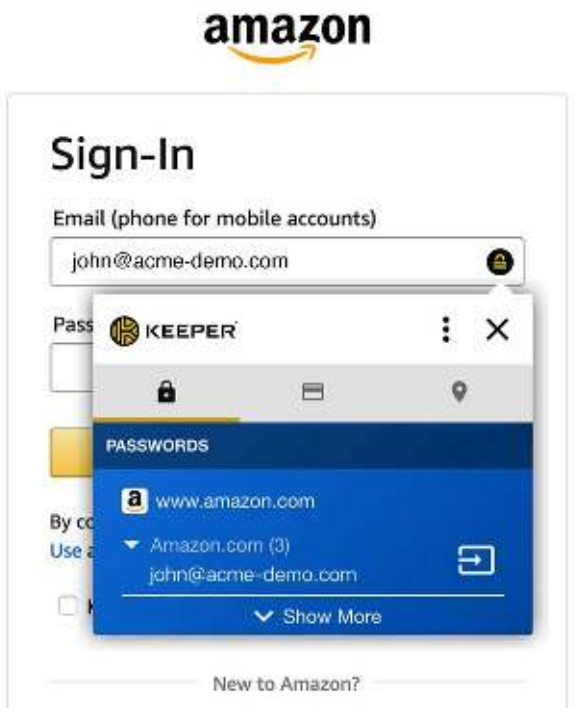


TrinWare
Hardware + Software + People

KeeperFill

- With KeeperFill, you can **autofill** your login credentials and save new website information to your secure Keeper vault. The KeeperFill browser extension is available for Chrome, Firefox, Safari, "Edge", Opera. To learn more about KeeperFill, check out our guides under KeeperFill Browser Extensions.





Security **Audit**

- The Security Audit feature gives you an overview of the passwords you have stored and gives you an idea of how secure your accounts are in total
- There are 3 categories for your stored passwords: All, Reused, and Weak
- The first two require no explanation, but a weak password is anything that can be easily guessed, or uses generic personal information that can be easily discovered such as a birthday or pet name

BreachWatch keeps a record of high-risk passwords and breaches that may have occurred

There is a category for Risks Found from Scans and Resolved History

The purpose of this feature is to allow you to be aware of and respond to security situations accordingly ASAP

BreachWatch

Additional Resources

For a more in-depth look into Keeper's features and how to's, here is the official user guide:
https://docs.keeper.io/user-guides/