

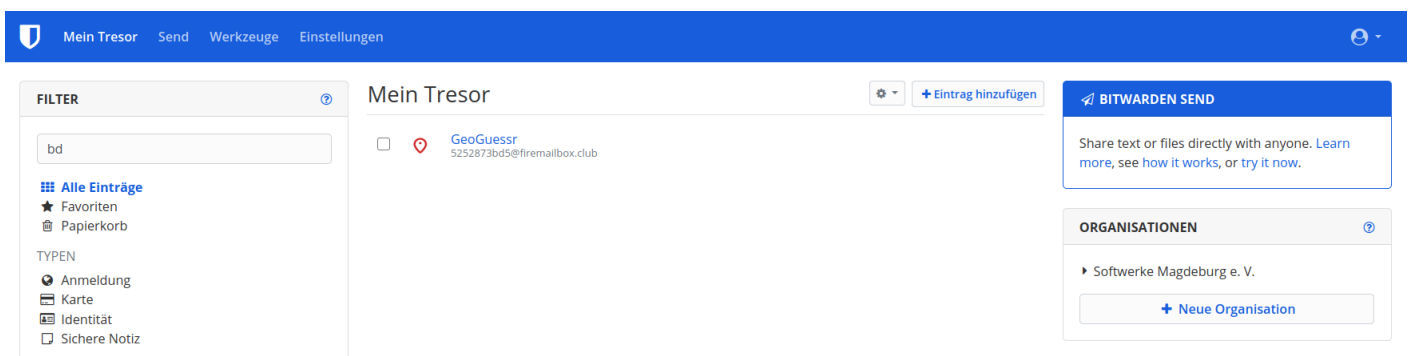
# Password-Vault

Auf jeder Seite soll man ein einmaliges, sicheres Passwort verwenden, am besten ein schwer zu merkendes, und dann soll man sich alle merken? Das geht nicht - Abhilfe schaffen Passwort-Manager, bei denen man mit einem Master-Passwort (plus optional weitere Sicherheitsmaßnahmen) einen verschlüsselten Tresor aufschließen kann, in dem man dann alle seine Accounts und Passwörter verwaltet.

Die Softwerke bieten dafür [BitWarden](#) (bzw. technisch gesehen [bitwarden\\_rs](#)) an, du findest es unter [vault.magdeburg.jetzt](#).

**Die Logindaten für deinen Tresor sind aus Sicherheitsgründen vollständig getrennt von deinem restlichen Softwerke-Account! Du benötigst jedoch einen Softwerke-Account mit der gleichen E-Mail-Adresse, um dich für den Tresor registrieren zu können.**

Ohne deinem Master-Passwort kann niemand auf deine Passwörter zugreifen, merke es dir darum sehr gut! Im Idealfall merkst du dir nur dein Master-Passwort für den Tresor und änderst dein Passwort für den Softwerke-Account direkt auf ein im Tresor generiertes & gespeichertes zufälliges Passwort.



## Einrichtung eines zweiten Faktors für mehr Sicherheit


In den Tresor-Einstellungen gibt es die Option "[Zwei-Faktor-Authentifizierung](#)" (2FA), wo du beispielsweise eine *Authentifizierungs-App* wie den [Aegis Authenticator](#) für Android oder den [Tofu Authenticator](#) für iOS als zweiten Faktor einrichten kannst. Sicherer sind jedoch *FIDO U2F-Sicherheitsschlüssel* - das sind kleine USB-Sticks (beispielsweise der [SoloKeys Solo V2](#) oder der [Nitrokey FIDO2](#)), die du zusammen mit deinem Passwort quasi wie einen klassischen "Schlüssel" zu deinem Tresor nutzen kannst.

Ein zweiter Faktor bedeutet, dass jemand der dein Passwort (den ersten Faktor) kennt, sich nur anmelden kann, wenn er auch Zugriff auf dein Handy oder deinen U2F-Schlüssel hat. Eine detailliertere Anleitung findest du unter "[Alles über Zwei-Faktor-Authentifizierung](#)".

Die Zwei-Faktor-Authentifizierung betrifft deinen Tresor nur logisch, nicht kryptografisch - das bedeutet, dass unsere AG Technik theoretisch trotz 2FA nur dein Master-Passwort benötigt, um deinen Tresor zu entschlüsseln. Es schützt jedoch sehr gut gegen viele mögliche Angriffe von außen und ist darum

unbedingt zu empfehlen.

## Nutzung auf anderen Webseiten & am Handy

Um die Passwörter auf Webseiten und in Apps zu nutzen, gibt es [auf der Webseite von BitWarden Apps und Browser-Erweiterungen](#) für die meisten Geräte. Hierbei musst du bei der Anmeldung oben links das Zahnrad  [Einstellungen](#) anklicken, und dort als "Server-URL" die Adresse `https://vault.softwerke.md` angeben: (vault statt tresor)

Schließen	Bitwarden	Speichern
SELBSTGEGHOSTETE UMGEBUNG		
Server URL		
<code>https://tresor.softwerke.md</code>		
Bitte gib die Basis-URL deiner selbst gehosteten Bitwarden-Installation an.		

## Sicherung und Backup

**Exportiere regelmäßig deine Passwort-Datenbank und sichere sie in deinem Backup.** Wir übernehmen keine Garantie, dass deine Passwörter nicht verloren gehen können. Im Team nutzen wir auch unsere Bitwarden-Instanz, daher haben wir aber selbst ein großes Interesse daran, dass nichts schief geht. Aber sichere so wichtige Sachen wie Passwörter bitte trotzdem nochmal unabgänglich von uns ab.

Um deinen Tresor zu exportieren, kannst du [hier klicken](#) oder in Bitwarden im Tab "Werkzeuge" > "Tresor exportieren" deine Daten exportieren. Falls du dir unsicher bist, wähle am besten als Dateiformat *json (Encrypted)*, damit die Datenbank auch auf deiner Festplatte vor unbefugtem Zugriff geschützt ist (z.B. falls dein Laptop verloren geht).



WERKZEUGE

Generator

Daten importieren

Tresor exportieren

## Tresor exportieren

### PERSÖNLICHER TRESOR WIRD EXPORTIERT

Es werden nur persönliche Tresoreinträge exportiert, die mit hanneskuehn@posteo.de verbunden sind. Tresoreinträge der Organisation werden nicht berücksichtigt. Es werden nur Informationen der Tresoreinträge exportiert. Diese enthalten nicht die zugehörigen Anhänge.

### Dateiformat

.json (Encrypted) ▾

### Exporttyp

☐ Konto eingeschränkt

Verwende den Verschlüsselungscode deines Kontos, abgeleitet vom Benutzernamen und Master-Passwort, um den Export zu verschlüsseln und den Import auf das aktuelle Bitwarden-Konto zu beschränken.

☒ Passwortgeschützt

Lege ein Dateipasswort fest, um den Export zu verschlüsseln und importiere ihn in ein beliebiges Bitwarden-Konto, wobei das Passwort zum Entschlüsseln genutzt wird.

### Dateipasswort (erforderlich)

Dieses Passwort wird verwendet, um diese Datei zu exportieren und zu importieren

### Dateipasswort bestätigen (erforderlich)

Format bestätigen

Version #23

Erstellt: 16 April 2021 06:43:17 von Moritz Marquardt

Zuletzt aktualisiert: 23 Januar 2024 19:03:46 von witziege