



Passwort-Tresor

LOKALER PASSWORT-MANAGER

Anleitung

Version 0.1.0 · © 2026 niederaastroth.de · Entwickelt von Volker Niederaastroth

Inhalt

- | | | | |
|---|---------------------------------------|----|-------------------------------|
| 1 | Willkommen | 10 | Frühere Passwörter |
| 2 | Installation und erster Start | 11 | Einstellungen |
| 3 | Den Tresor anlegen | 12 | Master-Passwort ändern |
| 4 | Sperren und Entsperren | 13 | Import, Export und Backup |
| 5 | Die Oberfläche im Überblick | 14 | Info-Fenster und eigene Links |
| 6 | Einträge anlegen und bearbeiten | 15 | Tastenkürzel |
| 7 | Passwörter benutzen | 16 | So ist der Tresor geschützt |
| 8 | 2FA-Codes (TOTP) | 17 | Passwort-Tresor oder Browser? |
| 9 | Sicherheits-Check und Datenleck-Check | 18 | Häufige Fragen |

Das Wichtigste vorweg

Dein Master-Passwort kann **nicht** zurückgesetzt oder wiederhergestellt werden – weder von dir noch vom Entwickler. Wer es vergisst, verliert alle gespeicherten Daten. Merke es dir gut, bewahre es sicher auf (zum Beispiel ausgedruckt im Safe) und lege regelmäßig ein verschlüsseltes Backup an (Kapitel 13).

1 Willkommen

Passwort-Tresor ist ein Passwort-Manager für Windows. Er speichert deine Zugangsdaten verschlüsselt auf deinem eigenen Rechner. Es gibt **keinen Server, kein Konto und keine Cloud** – die Daten verlassen deinen Computer nicht.

Was das Programm kann

- Zugangsdaten speichern: Titel, Website, Benutzername, Passwort, Kategorie, Notizen, Favorit
- Starke Zufallspasswörter erzeugen und die Stärke bewerten
- 2FA-Codes (TOTP) wie in einer Authenticator-App anzeigen
- Schwache, doppelt verwendete und alte Passwörter finden
- Passwörter auf Wunsch gegen bekannte Datenlecks prüfen (Have I Been Pwned)
- Zwischenablage automatisch leeren, Tresor automatisch sperren
- Aus Chrome, Edge oder Bitwarden importieren, verschlüsselte Backups anlegen
- Bedienung auf Deutsch und Englisch

Was es bewusst nicht gibt

- Keine Synchronisation zwischen Geräten und kein automatisches Ausfüllen im Browser. Zum Umzug auf einen anderen Rechner kopierst du eine Backup-Datei.
- Keine Passwort-Wiederherstellung. Das ist die Folge der starken Verschlüsselung, siehe Kapitel 16.

2 Installation und erster Start

- 1 Starte `Passwort-Tresor Setup x.y.z.exe` und wähle den Zielordner. Eine Administrator-Installation ist nicht nötig, das Programm wird für deinen Benutzer installiert.
- 2 Windows zeigt eventuell die Warnung „Der Computer wurde durch Windows geschützt“ (SmartScreen), weil das Installationsprogramm nicht digital signiert ist. Klicke auf *Weitere Informationen* und dann auf *Trotzdem ausführen*.
- 3 Starte „Passwort-Tresor“ über das Startmenü oder die Desktop-Verknüpfung.

Das Programm läuft nur einmal gleichzeitig: Ein zweiter Start holt das vorhandene Fenster nach vorn.

Wo liegen die Daten?

```
%APPDATA%\Passwort-Tresor\vault.pwm
```

Das ist dein verschlüsselter Tresor. Daneben liegt `vault.pwm.bak` (der Stand vor der letzten Änderung) und `prefs.json` (die gewählte Sprache). Die Sprache folgt zunächst der Windows-Einstellung und lässt sich jederzeit umstellen (Kapitel 11).

3 Den Tresor anlegen

Beim ersten Start legst du den Tresor an. Dafür vergibst du ein **Master-Passwort**. Es ist der einzige Schlüssel zu allen deinen Daten.

Abb. 1 – Neuen Tresor anlegen: Master-Passwort eingeben, wiederholen, „Tresor erstellen“

- 1 Gib das Master-Passwort ein. Der Balken darunter zeigt die geschätzte Stärke.
- 2 Wiederhole es im zweiten Feld.
- 3 Klicke auf *Tresor erstellen*. Das dauert einen kurzen Moment, weil der Schlüssel bewusst aufwendig berechnet wird.

Anforderungen an das Master-Passwort

- mindestens 10 Zeichen,
- nicht zu vorhersehbar – das Programm lehnt Passwörter wie „Sommer2024“ oder „12345678“ ab.

Tipp: Merksatz statt Zeichensalat

Vier bis fünf zufällige, nicht zusammenhängende Wörter mit ein paar Ziffern sind stark und leicht zu merken, zum Beispiel `Kaffee-Tasse-Sonnenuntergang-42`. Nimm keinen Satz aus einem Lied, Zitat oder deinem Umfeld.

Es gibt keine „Passwort vergessen“-Funktion

Wer das Master-Passwort verliert, kommt nie wieder an die Daten – auch der Entwickler nicht. Notiere es und bewahre es an einem sicheren Ort auf, getrennt vom Rechner.

Hast du schon ein Backup eines früheren Tresors, kannst du es hier über *Vorhandenes Backup wiederherstellen* einspielen (Kapitel 13).

4 Sperren und Entsperren

Ist der Tresor gesperrt, liegen die Daten nur verschlüsselt vor. Zum Arbeiten entsperrst du ihn mit dem Master-Passwort.

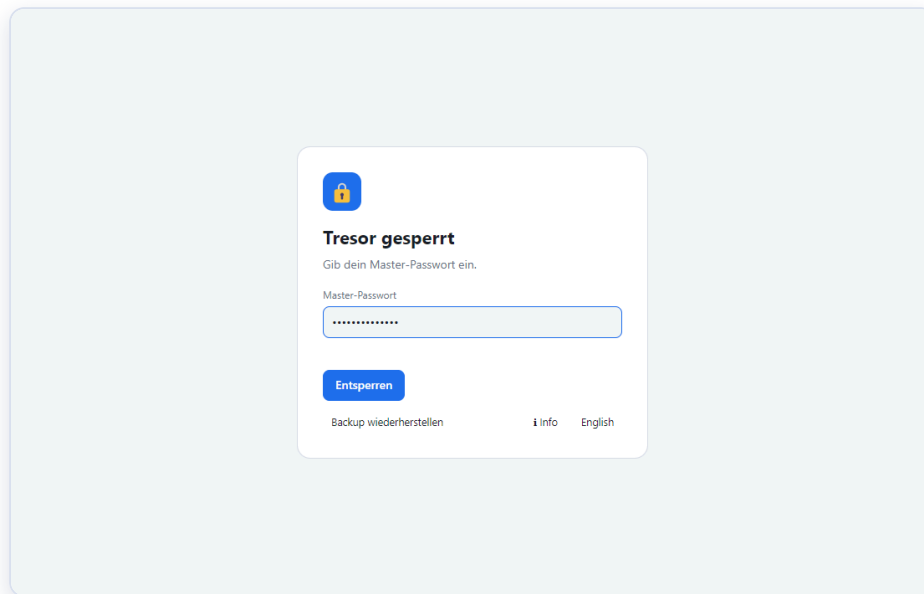


Abb. 2 – Der Sperrbildschirm

Wann sperrt der Tresor?

Auslöser	Hinweis
Knopf  Sperren oder Strg + L	sofort, von Hand
Keine Bedienung	nach 5 Minuten (einstellbar von 1 Minute bis 1 Stunde oder nie)
Fenster minimieren	einstellbar, standardmäßig an
Windows-Sperrbildschirm oder Standby	immer

Beim Sperren wird auch die Zwischenablage geleert, wenn sie noch ein von hier kopiertes Passwort enthält. Der Sperrbildschirm nennt den Grund, zum Beispiel „Automatisch gesperrt (Inaktivität)“.

Fehlversuche

Nach mehreren falschen Passwörtern wird die nächste Prüfung künstlich verzögert (bis zu 10 Sekunden). Das bremst automatisches Durchprobieren.

5 Die Oberfläche im Überblick

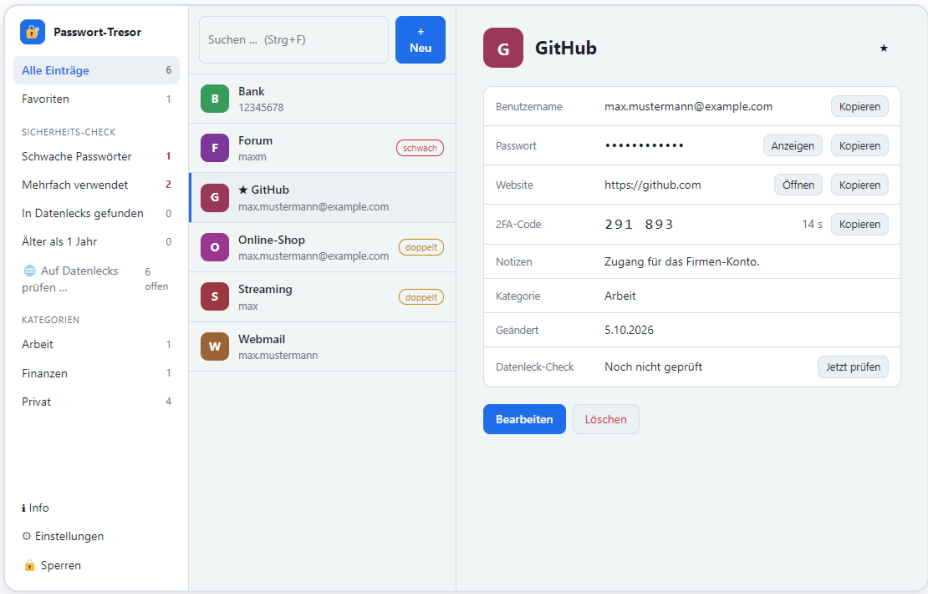


Abb. 3 – Seitenleiste, Liste und Detailansicht

Bereich	Inhalt
Links: Seitenleiste	Filter <i>Alle Einträge</i> und <i>Favoriten</i> ; der <i>Sicherheits-Check</i> mit Zählern; deine <i>Kategorien</i> ; unten <i>Info</i> , <i>Einstellungen</i> und <i>Sperren</i>
Mitte: Liste	Suchfeld (Strg + F) und Knopf + <i>Neu</i> . Farbige Marken zeigen Probleme: „schwach“, „doppelt“, „geleakt“
Rechts: Detailansicht	Alle Felder des gewählten Eintrags mit Knöpfen zum Kopieren, Anzeigen und Öffnen

Die Suche durchsucht Titel, Website, Benutzername und Kategorie. Ein Stern vor dem Titel kennzeichnet Favoriten.

Leerer Tresor

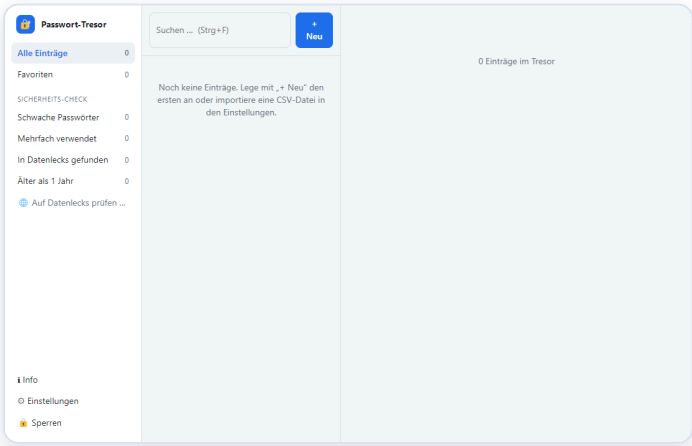


Abb. 4 – Ein neuer Tresor ist leer

6 Einträge anlegen und bearbeiten

Klicke auf + *Neu* (oder **Strg** + **N**). Zum Ändern wählst du einen Eintrag und klickst auf *Bearbeiten*.

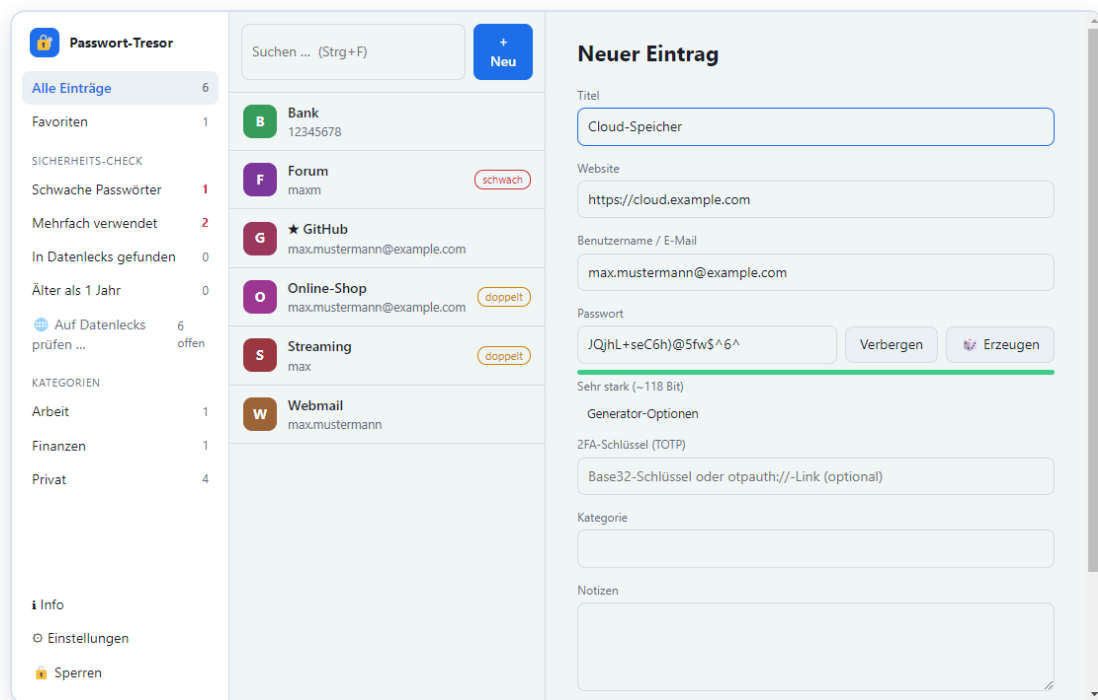


Abb. 5 – Das Formular für einen neuen Eintrag

Feld	Bedeutung
Titel	Pflichtfeld, so heißt der Eintrag in der Liste
Website	Adresse der Seite; wird für den Knopf <i>Öffnen</i> benutzt
Benutzername / E-Mail	Login-Name
Passwort	mit Stärke-Anzeige; <i>Anzeigen</i> blendet es ein,  <i>Erzeugen</i> würfelt ein neues
2FA-Schlüssel (TOTP)	optional, siehe Kapitel 8
Kategorie	freier Name; bereits benutzte Kategorien werden vorgeschlagen und erscheinen in der Seitenleiste
Notizen	freier Text, wird nur als Text angezeigt
Favorit	markiert den Eintrag mit einem Stern

Ein **neuer** Eintrag startet gleich mit einem erzeugten, starken Passwort. Mit *Speichern* übernimmst du alles, mit *Abbrechen* oder **Esc** verwirfst du die Änderungen.

Der Passwort-Generator

Ein Klick auf *Generator-Optionen* öffnet die Einstellungen des Generators. Sie bleiben für die nächsten Passwörter erhalten, solange das Programm läuft.

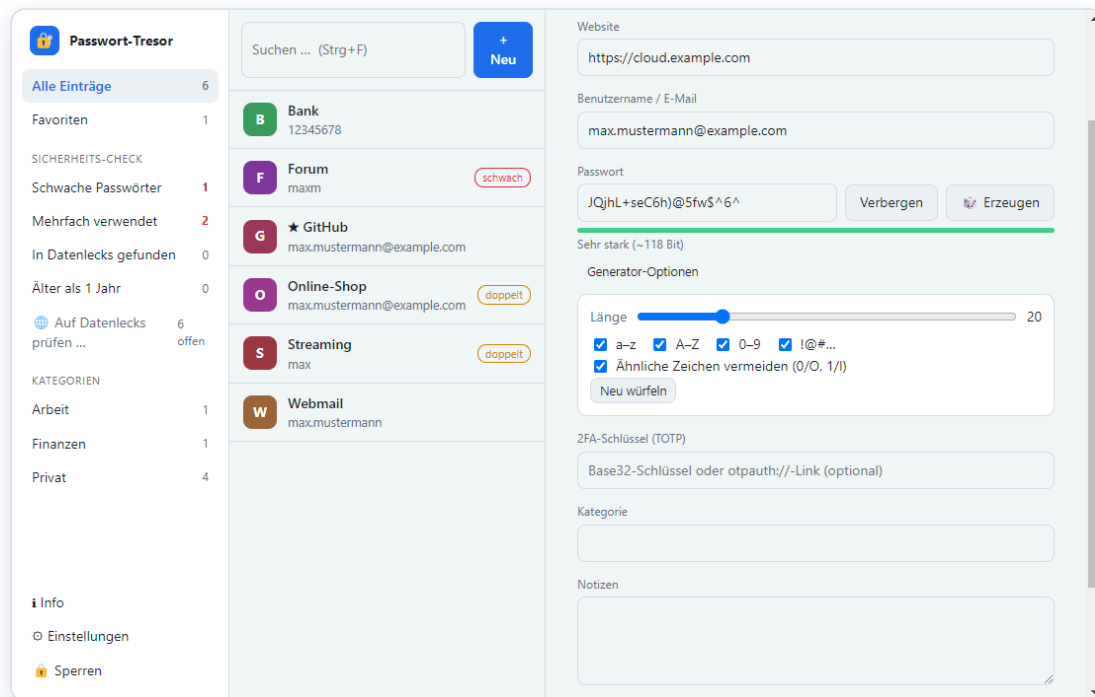


Abb. 6 – Länge und Zeichenarten des Generators

- **Länge:** 8 bis 64 Zeichen (Standard 20).
- **Zeichenarten:** Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen. Jede gewählte Art kommt mindestens einmal vor.
- **Ähnliche Zeichen vermeiden:** lässt Zeichen wie 0/O und 1/I weg, die sich leicht verwechseln lassen.
- **Neu würfeln:** erzeugt sofort ein neues Passwort mit den gewählten Optionen.

Tipp

Für jede Website ein eigenes, zufälliges Passwort mit mindestens 16 Zeichen. Du musst es dir nicht merken – dafür ist der Tresor da.

7 Passwörter benutzen

In der Detailansicht eines Eintrags stehen neben jedem Feld Knöpfe:

Knopf	Wirkung
<i>Kopieren</i>	legt Benutzername, Passwort, Adresse oder 2FA-Code in die Zwischenablage. Ein Hinweis nennt, wann sie wieder geleert wird
<i>Anzeigen / Verbergen</i>	zeigt das Passwort im Klartext oder blendet es wieder aus
<i>Öffnen</i>	öffnet die Website im Standardbrowser (nur http- und https-Adressen)
Stern oben rechts	Favorit setzen oder entfernen
<i>Löschen</i>	entfernt den Eintrag nach Rückfrage endgültig

Das übliche Vorgehen: Seite öffnen, *Benutzername kopieren*, einfügen, dann *Passwort kopieren* und einfügen. Die Zwischenablage wird nach der eingestellten Zeit (Standard 20 Sekunden) automatisch geleert, aber nur, wenn noch dein kopiertes Passwort darin liegt.

Windows-Zwischenablageverlauf

Ist der Verlauf der Zwischenablage (**Win** + **V**) eingeschaltet, kann Windows kopierte Passwörter trotz automatischem Leeren speichern. Schalte ihn in den Windows-Einstellungen unter *System* → *Zwischenablage* aus, wenn du das nicht möchtest.

8 2FA-Codes (TOTP)

Viele Dienste verlangen zusätzlich zum Passwort einen Code aus einer Authenticator-App. Passwort-Tresor kann diese Codes selbst erzeugen (Verfahren nach RFC 6238, kompatibel mit Google Authenticator & Co.).

Einrichten

- 1 Aktiviere beim Dienst die Zwei-Faktor-Anmeldung mit einer Authenticator-App. Der Dienst zeigt einen QR-Code und meist auch den Schlüssel als Text (Base32, Buchstaben und Ziffern).
- 2 Kopiere den Schlüssel in das Feld *2FA-Schlüssel (TOTP)* deines Eintrags. Alternativ geht ein `otpauth://`-Link.
- 3 Speichere den Eintrag. In der Detailansicht erscheint der aktuelle **2FA-Code** mit Restzeit; er wechselt alle 30 Sekunden.

Mit *Kopieren* legst du den aktuellen Code in die Zwischenablage. Ist der Schlüssel fehlerhaft, steht „Ungültiger 2FA-Schlüssel“ statt eines Codes.

Beachte

Liegen Passwort und 2FA-Schlüssel im selben Tresor, schützt die Zwei-Faktor-Anmeldung nicht mehr vor einem Angreifer, der den Tresor öffnet. Sie schützt weiterhin gegen gestohlene oder geleakte Passwörter. Bewahre für wichtige Konten die Wiederherstellungscodes des Dienstes separat auf.

9 Sicherheits-Check und Datenleck-Check

In der Seitenleiste zeigt der Bereich *Sicherheits-Check*, wo Handlungsbedarf besteht. Ein Klick auf den Eintrag filtert die Liste.

Filter	Bedeutet
Schwache Passwörter	Die geschätzte Stärke ist niedrig (unter ca. 45 Bit)
Mehrfach verwendet	Dasselbe Passwort steht in mehreren Einträgen
In Datenlecks gefunden	Das Passwort tauchte in bekannten Datenlecks auf (nach einer Prüfung)
Älter als 1 Jahr	Das Passwort wurde seit über einem Jahr nicht geändert

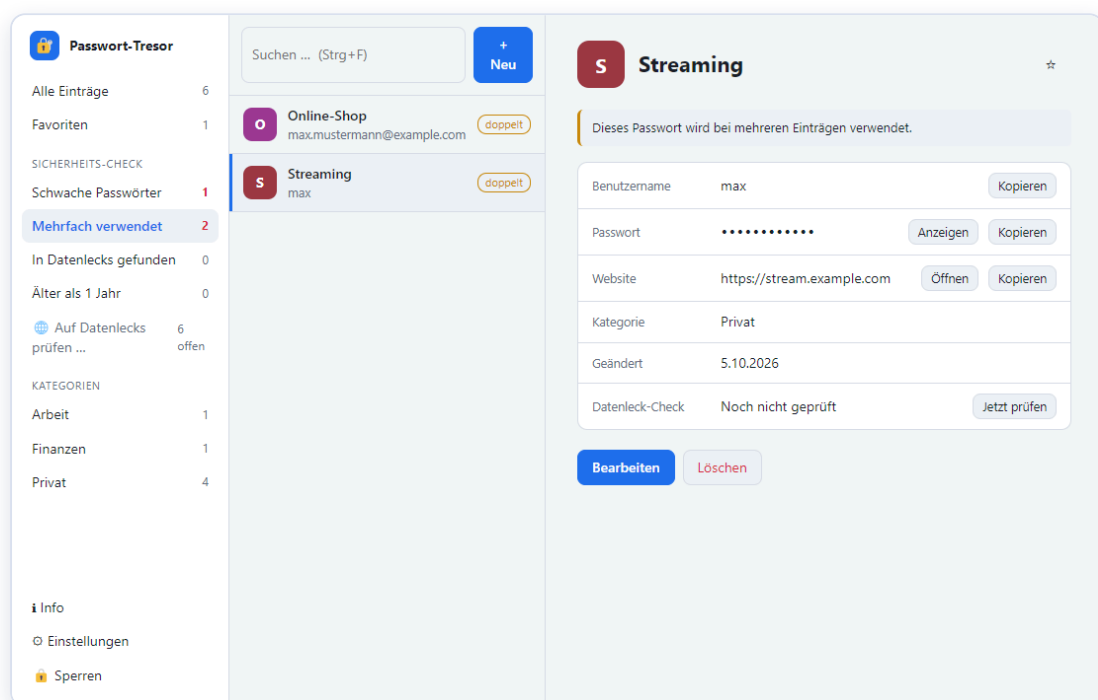


Abb. 7 – Filter „Mehrfach verwendet“: zwei Einträge teilen sich ein Passwort

Ändere solche Passwörter beim jeweiligen Dienst und trage das neue im Eintrag ein (*Bearbeiten* → 🎲 *Erzeugen*).

Datenleck-Check

Mit 🌐 *Auf Datenlecks prüfen ...* in der Seitenleiste prüfst du alle Passwörter, mit *Jetzt prüfen* in der Detailansicht nur das eines Eintrags. Das Programm fragt vorher um Erlaubnis.

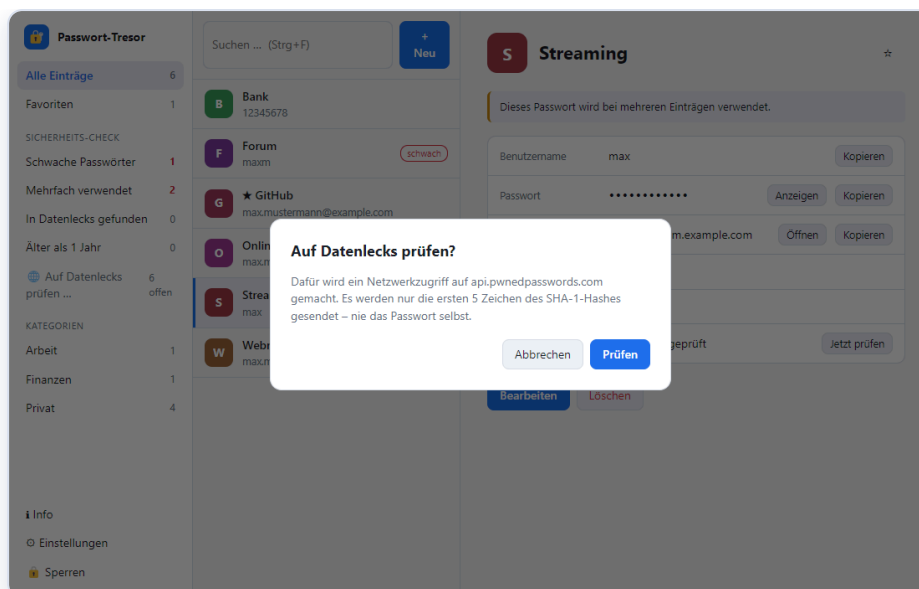


Abb. 8 – Rückfrage vor dem Netzwerkzugriff

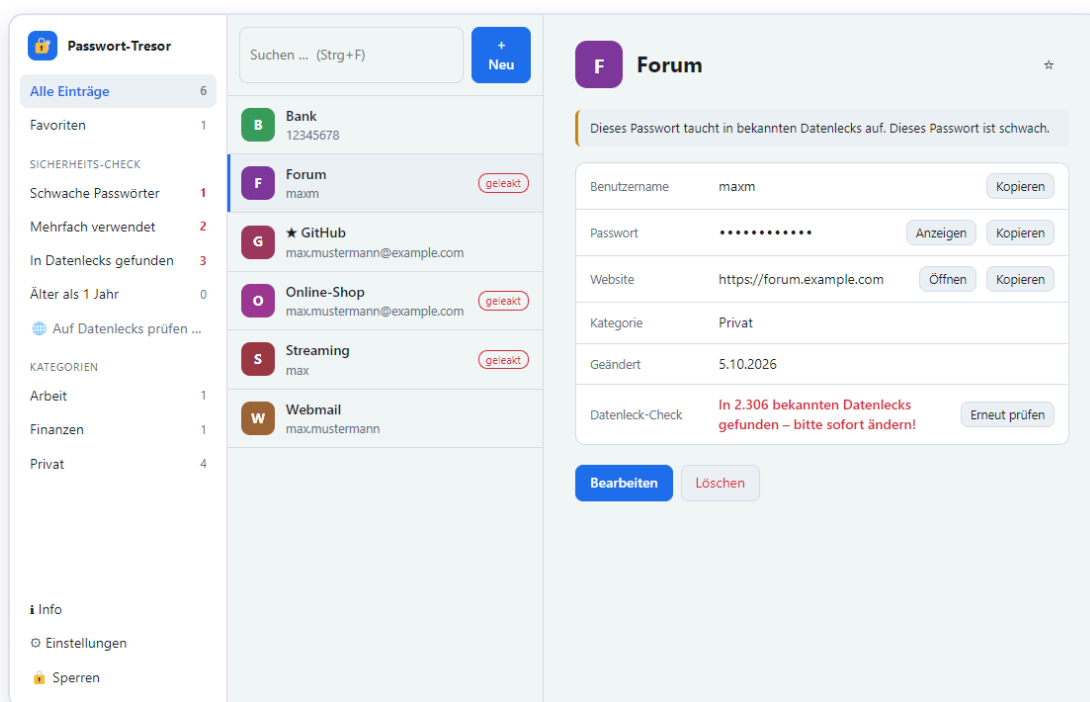


Abb. 9 – Ergebnis: „Sommer2024“ steht in 2.306 bekannten Datenlecks

Datenschutz

Es wird nie dein Passwort gesendet. Das Programm bildet einen SHA-1-Hashwert und schickt nur dessen **ersten 5 Zeichen** an den Dienst `api.pwnedpasswords.com`. Der Dienst liefert alle passenden Treffer zurück, der Vergleich geschieht auf deinem Rechner. Es ist die einzige Netzanfrage des Programms und läuft nur nach deiner Bestätigung.

Ein Treffer heißt: Das Passwort ist öffentlich bekannt und wird bei Angriffen ausprobiert. Ändere es sofort. „Nicht gefunden“ bedeutet nicht automatisch „sicher“, aber es ist ein gutes Zeichen. Wird ein Passwort geändert, gilt das alte Prüfergebnis nicht mehr.

10 Frühere Passwörter

Ändert man das Passwort eines Eintrags, merkt sich der Tresor die bisherigen (bis zu 10). Das hilft, wenn ein Dienst die Änderung nicht angenommen hat oder du ein altes Passwort für ein Archiv brauchst.

In der Detailansicht erscheint dann die Zeile *Frühere Passwörter* mit dem Knopf *Anzeigen*.

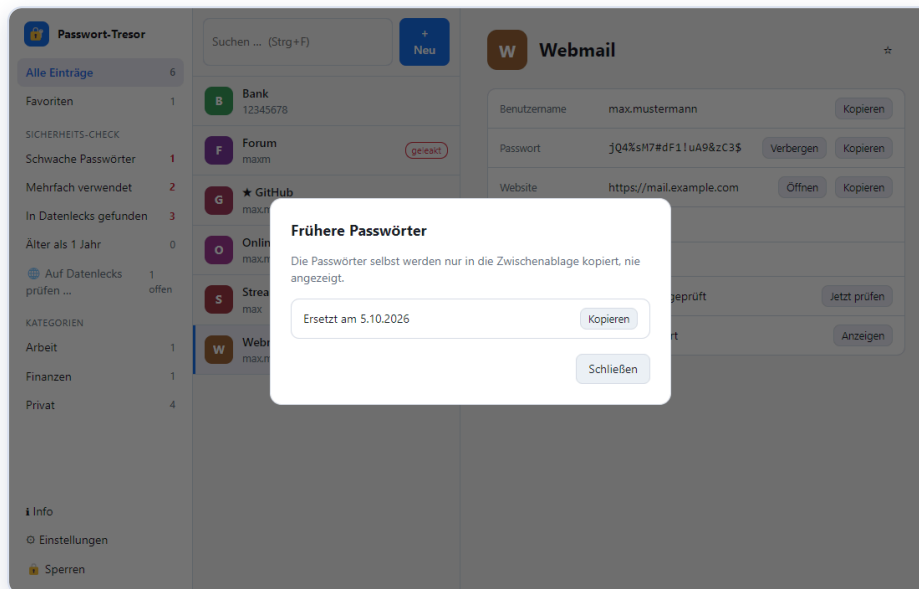


Abb. 10 – Liste früherer Passwörter mit Änderungsdatum

Aus Sicherheitsgründen werden alte Passwörter **nicht angezeigt**, sondern nur mit *Kopieren* in die Zwischenablage gelegt.

11 Einstellungen

Die Einstellungen öffnest du mit  *Einstellungen* in der Seitenleiste. Änderungen gelten sofort. Die Sicherheits-Einstellungen werden im Tresor gespeichert, die Sprache in `prefs.json`.

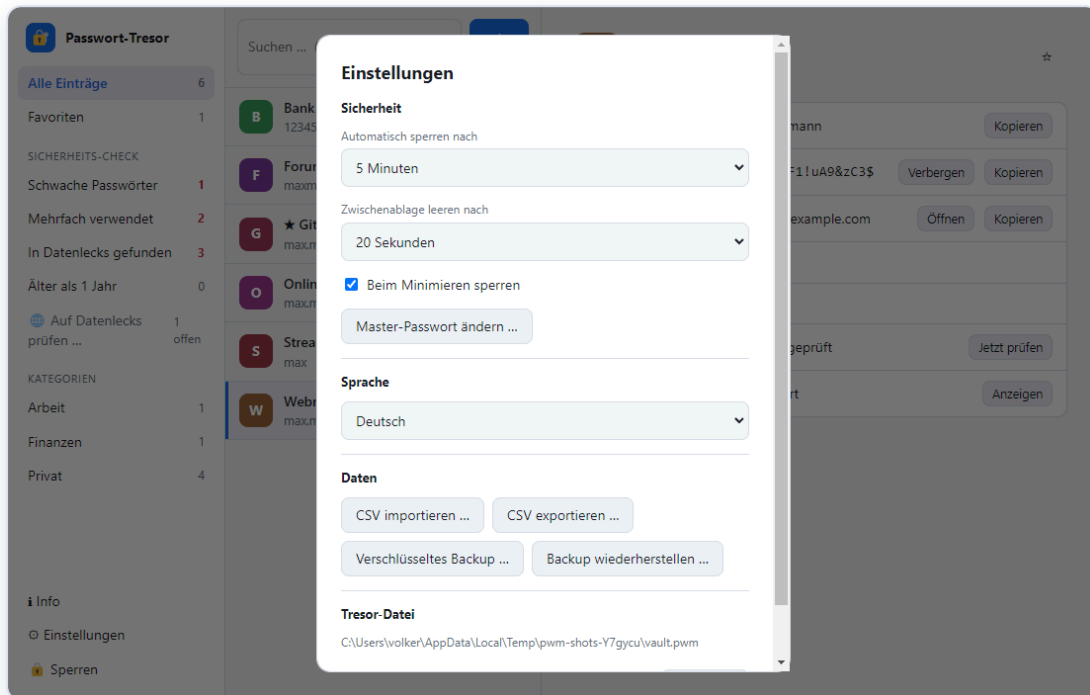


Abb. 11 – Einstellungen

Einstellung	Auswahl (Standard fett)
Automatisch sperren nach	Nie, 1, 2, 5 , 10, 15, 30 Minuten, 1 Stunde
Zwischenablage leeren nach	Nie, 10, 20 , 30, 60 Sekunden
Beim Minimieren sperren	an / aus
Sprache	Deutsch / English (wirkt sofort, auch auf Dialoge)

Außerdem findest du hier das *Master-Passwort ändern*, die Daten-Funktionen (Kapitel 13) und den Speicherort der Tresor-Datei.

12 Master-Passwort ändern

Du kannst das Master-Passwort jederzeit ändern, zum Beispiel wenn du glaubst, dass jemand es kennt.

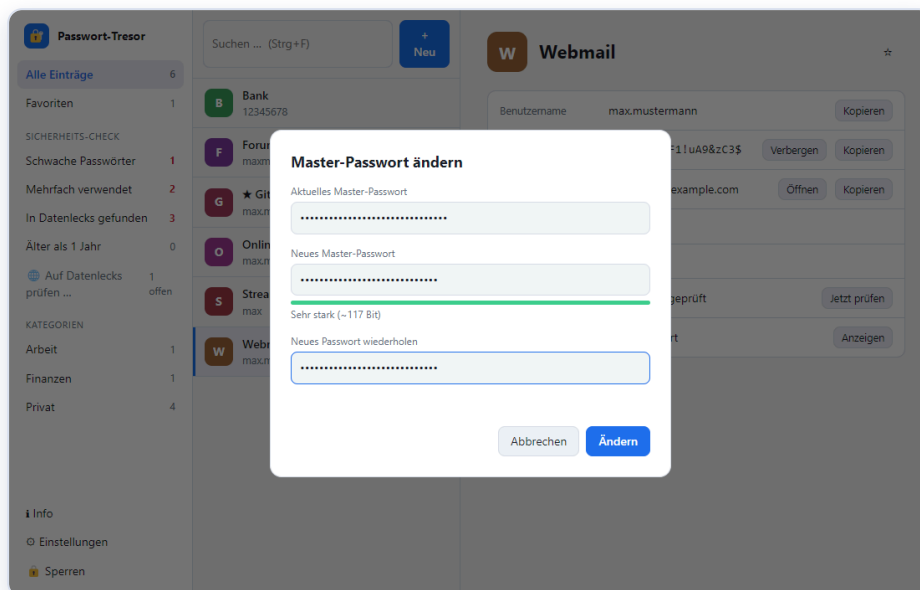


Abb. 12 – Master-Passwort ändern

- 1 Öffne *Einstellungen* → *Master-Passwort ändern*
- 2 Gib das aktuelle Passwort ein, dann zweimal das neue.
- 3 Klicke auf *Ändern*. Der Tresor wird mit einem neuen Schlüssel neu verschlüsselt.

Alte Backups behalten das alte Passwort

Ein Backup lässt sich nur mit dem Master-Passwort öffnen, das beim Erstellen galt. Lege nach einer Änderung ein neues Backup an und notiere dir, welches Passwort zu welchem Backup gehört.

13 Import, Export und Backup

Alle Funktionen findest du in den Einstellungen im Bereich *Daten*.

CSV importieren

Exportiere die Passwörter aus Chrome, Edge, Bitwarden oder einem anderen Programm als CSV-Datei und wähle *CSV importieren* Spalten wie `name`, `url`, `username`, `password`, `note` werden erkannt. Einträge, die schon existieren, werden übersprungen. Danach nennt das Programm, wie viele Einträge importiert wurden.

Lösche die CSV-Datei sofort nach dem Import

Sie enthält alle Passwörter im Klartext. Leere auch den Papierkorb, und entferne die Passwörter anschließend aus dem Browser, wenn du ihn nicht mehr dafür nutzen willst.

CSV exportieren

CSV exportieren ... speichert alle Einträge als Klartext-Datei, etwa zum Wechsel zu einem anderen Programm. Vorher erscheint eine Warnung, die du bestätigen musst. Nutze diese Funktion nur, wenn nötig, speichere die Datei an einem sicheren Ort und lösche sie nach Gebrauch.

Verschlüsseltes Backup

Verschlüsseltes Backup ... speichert eine Kopie des Tresors als `.pwm`-Datei. Sie ist genauso verschlüsselt wie der Tresor selbst und darf deshalb auf einem USB-Stick oder in einem Cloud-Ordner liegen. Der Dateiname enthält das Datum, zum Beispiel `vault-backup-2026-10-05.pwm`.

Backup wiederherstellen

- 1 Wähle *Backup wiederherstellen* ... (auch auf dem Sperr- und Einrichtungsbildschirm möglich) und die `.pwm`-Datei.
- 2 Bestätige die Rückfrage. Der aktuelle Tresor wird ersetzt, der bisherige bleibt als `vault.pwm.before-restore.bak` erhalten.
- 3 Entsperre danach mit dem Master-Passwort **des Backups**.

Backup-Gewohnheit

Lege nach größeren Änderungen und mindestens einmal im Monat ein Backup an – am besten an zwei verschiedenen Orten. Auf einem neuen Rechner installierst du das Programm und spielst auf dem Einrichtungsbildschirm das Backup ein.

14 Info-Fenster und eigene Links

Das Info-Fenster öffnest du mit **i Info** in der Seitenleiste, auf dem Sperrbildschirm oder mit **F1**. Es funktioniert auch bei gesperrtem Tresor.

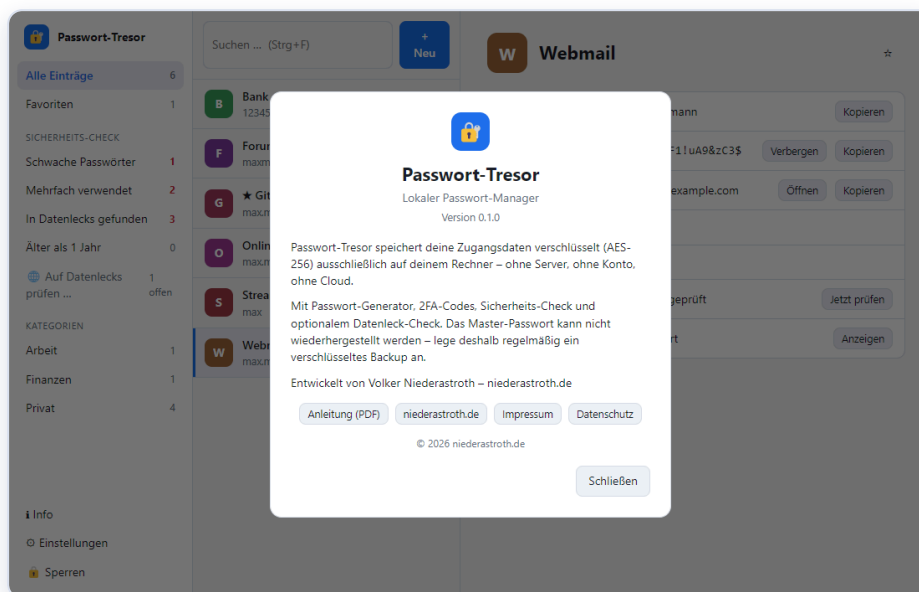


Abb. 13 – Das Info-Fenster mit Version, Beschreibung und Links

Text und Links ändern

Titel, Text, Links und Copyright stehen in zwei Textdateien, die du mit jedem Editor ändern kannst:

Sprache	Datei
Deutsch	about.json
Englisch	about.en.json

Sie liegen im Programmordner:

```
%LOCALAPPDATA%\Programs\Passwort-Tresor\Resources\
```

- 1 Öffne die Datei in einem Editor (zum Beispiel Notepad).
- 2 Ändere nur die Werte in Anführungszeichen. Kommas und Klammern müssen stehen bleiben.
- 3 Speichere und starte das Programm neu.

Aufbau der Datei

```
{
  "title": "Passwort-Tresor",
  "subtitle": "Lokaler Passwort-Manager",
  "text": [ "Erster Absatz ...", "Zweiter Absatz ..." ],
  "links": [
    { "label": "Meine Website", "url": "https://www.example.com/" },
    { "label": "Anleitung (PDF)", "file": "Passwort-Tresor-Anleitung.pdf" }
  ],
  "copyright": "© 2026 Beispiel"
}
```

- `"url"` öffnet eine Web-Adresse im Browser (nur `http://` und `https://`).
- `"file"` öffnet ein PDF, das im selben Ordner wie die JSON-Datei liegt.
- Weitere Absätze oder Links ergänzt du einfach als zusätzliche Einträge in den Listen.

Beachte

Ein Programm-Update überschreibt diese Dateien mit den mitgelieferten Fassungen. Hebe dir deine Änderungen deshalb zusätzlich auf. Ist die Datei fehlerhaft (zum Beispiel ein Komma vergessen), bleibt das Info-Fenster leer, und das Programm läuft normal weiter.

15 Tastenkürzel

Taste	Wirkung
Strg + F	Suchfeld aktivieren
Strg + N	Neuer Eintrag
Strg + L	Tresor sperren
F1	Info-Fenster
Esc	Dialog schließen bzw. Bearbeiten abbrechen

16 So ist der Tresor geschützt

- **Verschlüsselung:** AES-256-GCM. Der Schlüssel entsteht mit scrypt ($N = 2^{17}$) aus dem Master-Passwort. Das macht jeden Rateversuch teuer.
- **Manipulationsschutz:** Eine veränderte oder beschädigte Datei wird erkannt und abgelehnt.
- **Kein Klartext auf der Festplatte:** Entschlüsselte Daten existieren nur im Arbeitsspeicher, solange der Tresor entsperrt ist. Beim Sperren wird der Schlüssel verworfen.
- **Sparsame Oberfläche:** Die Liste enthält keine Passwörter. Passwörter und 2FA-Schlüssel erreichen die Anzeige nur, wenn du sie ausdrücklich ansiehst oder bearbeitest.
- **Abgeschottetes Fenster:** Die Oberfläche hat keinen Netzwerkzugriff; Anfragen laufen nur im Hauptprogramm.
- **Sichere Dateiablage:** Speichern erfolgt über eine temporäre Datei, der vorherige Stand bleibt als `.bak` erhalten.

Grenzen

- Auf einem Rechner mit Schadsoftware (zum Beispiel Keylogger) kann kein Passwort-Manager schützen.
- Solange der Tresor entsperrt ist, liegen die Daten im Arbeitsspeicher des Programms.
- Der Windows-Zwischenablageverlauf kann kopierte Passwörter behalten (Kapitel 7).
- Ein schwaches Master-Passwort bleibt ein Risiko, wenn jemand Zugriff auf die Tresor-Datei bekommt.

17 Passwort-Tresor oder Browser?

Chrome, Edge und Firefox haben einen eigenen Passwort-Speicher. Dieses Kapitel hilft bei der Entscheidung, was für dich besser passt. Die Angaben zu den Browsern sind allgemein gehalten; Einzelheiten hängen von Version und Einstellungen ab.

Kriterium	Passwort-Tresor	Browser (Chrome / Edge)
Speicherort	Eine Datei auf deinem PC, keine Cloud	Im Browser-Profil, meist zusätzlich mit dem Browser-Konto synchronisiert
Schutz der Daten	Schlüssel wird aus deinem Master-Passwort berechnet (AES-256-GCM, scrypt). Ohne das Passwort ist die Datei wertlos	Schlüssel ist an dein Windows-Benutzerkonto gebunden. Wer dein entsperres Windows oder Konto übernimmt, kommt oft ohne weitere Hürde heran
Zusätzliche Hürde	Immer: Master-Passwort, dazu Auto-Sperre	Meist keine eigene Hürde, optional eine Windows-Abfrage beim Anzeigen
Schadsoftware	Schützt nur, solange der Tresor gesperrt ist. Entsperrt ist bei Schadsoftware alles lesbar	Browser-Passwörter sind ein beliebtes Ziel von Schadsoftware, auch wenn neuere Versionen es erschweren
Automatisches Ausfüllen	Nein, Kopieren und Einfügen	Ja, sehr bequem
Phishing-Schutz	Kein Ausfüllen, also achtest du selbst auf die Adresse	Füllt nur auf der gespeicherten Domain aus und schützt so vor vielen Fake-Seiten
Geräte, Handy	Nur dieser PC, Umzug per Backup-Datei	Alle Geräte mit demselben Konto, auch Handy
Passkeys	Nein	Ja
2FA-Codes	Ja, eingebaut	Meist nein
Zwischenablage	Wird automatisch geleert	Nicht nötig, es wird ausgefüllt
Sicherheits-Check	Schwach, doppelt, alt; Datenleck-Check auf Klick	Datenleck-Warnung, oft im Hintergrund
Datenschutz	Kein Server; Netzwerk nur beim Datenleck-Check auf Klick (5 Hash-Zeichen)	Daten liegen beim Browser-Anbieter, sofern die Synchronisierung an ist
Konto nötig	Nein	Meist ja (Google bzw. Microsoft)
Passwort vergessen	Keine Wiederherstellung	Über das Browser-Konto möglich

Kriterium	Passwort-Tresor	Browser (Chrome / Edge)
Notizen, Kategorien, Verlauf	Ja	Eingeschränkt oder nein
Reife	Neu (Version 0.1.0), nicht von Dritten geprüft	Millionenfach im Einsatz, laufend gewartet

Wann der Passwort-Tresor besser passt

- Du willst keine Passwörter bei Google oder Microsoft ablegen.
- Auch auf einem laufenden, entsperrten Windows soll der Zugriff ein Master-Passwort verlangen.
- Du willst 2FA-Codes, Notizen und Kategorien an einem Ort.

Wann der Browser besser passt

- Du brauchst Bequemlichkeit und Ausfüllen auf PC und Handy.
- Dir ist der Schutz durch automatisches Ausfüllen vor Fake-Seiten wichtig.
- Du willst Passkeys nutzen.

Firefox bietet ein „Hauptpasswort“, das dem Tresor-Prinzip ähnelt. Es ist standardmäßig ausgeschaltet.

Empfehlung

Für die wichtigsten Konten (Bank, E-Mail) bietet sich eine Kombination an: Passwörter im Tresor, dazu überall, wo möglich, die Zwei-Faktor-Anmeldung. Speichere ein Passwort nicht doppelt in Tresor *und* Browser, sonst hast du zwei Orte, die geschützt werden müssen. Hast du bisher Browser-Passwörter, kannst du sie als CSV in den Tresor importieren (Kapitel 13) und danach im Browser löschen.

18 Häufige Fragen

Ich habe das Master-Passwort vergessen. Was nun?

Es gibt keinen Weg zurück. Probiere Varianten, die du früher benutzt hast. Hast du ein älteres Backup und kennst das damals gültige Passwort, kannst du dieses Backup einspielen. Danach hilft nur ein neuer, leerer Tresor. Lege deshalb Backups an und bewahre das Passwort sicher auf.

Wie ziehe ich auf einen neuen Rechner um?

Lege am alten Rechner ein verschlüsseltes Backup an, kopiere die `.pwm`-Datei hinüber, installiere das Programm und spiele auf dem Einrichtungsbildschirm das Backup ein. Entsperre mit dem bisherigen Master-Passwort.

Kann ich den Tresor auf zwei Rechnern gleichzeitig benutzen?

Eine automatische Synchronisation gibt es nicht. Wer die Datei von Hand zwischen Rechnern kopiert, riskiert, Änderungen zu überschreiben. Arbeite besser auf einem Rechner und übertrage per Backup.

Warum fragt das Programm vor der Datenleck-Prüfung?

Weil es dafür das Internet benutzt. Das Programm sendet nie ohne dein Einverständnis etwas ins Netz (Kapitel 9).

Die Zwischenablage wurde zu früh geleert.

Erhöhe die Zeit unter *Einstellungen* → *Zwischenablage leeren nach*.

Das Info-Fenster ist leer.

Die Datei `about.json` fehlt oder enthält einen Fehler, zum Beispiel ein vergessenes Komma. Prüfe sie mit einem JSON-Prüfer oder kopiere die Originaldatei aus dem Installationsprogramm zurück (Kapitel 14).

Wo bekomme ich Hilfe?

Über die Links im Info-Fenster erreichst du den Entwickler: niederastroth.de.