Handbuch

Keyfiler for Web

Version 1.0.19

Stand: November 2026

> Die aktuelle Hilfe findest du jederzeit in der App mit F1 oder über das Fragezeichen. Fragen und Wünsche: info@keyfiler.com

Inhalt

1 Erste Schritte

- Konto einrichten
- Dein Name
- Wiederherstellungsschlüssel
- Zwei-Faktor-Anmeldung einrichten
- Entsperren mit Passkey
- Keyfiler als App installieren
  - Windows, Mac & Linux: Chrome und Edge
  - Mac: Safari
  - Firefox
  - Android
  - iPhone & iPad
  - App wieder entfernen

2 Tresore und Ordner

- Tresore anlegen und Kategorien
- Tresore mit anderen teilen
- Teilen per Link
- Ordner anlegen und sortieren
- Papierkorb

3 Vorsorge

- Vorsorgeordner
- Notfallzugang

4 Dokumente

- Aufbau eines Dokuments
- Dokumentvorlagen
- Anhänge
- 2FA-Codes in Dokumenten
- Passwort-Generator
- Termine

5 Schneller arbeiten

- Schnellzugriff und Favoriten
- Switchboard
- Suchen
- Tastenkürzel
- Neuigkeiten
- Hell und dunkel

6 Sicherheit

- Sicherheits-Check
- Passwort-Check
- Automatisches Sperren
- So schützt Keyfiler deine Daten
- Sicher unterwegs

7 Sichern und Übertragen

- Backup erstellen und wiederherstellen
- Daten aus der Desktop-Version übernehmen
- Aus anderen Passwortmanagern importieren
- Mehrere Geräte gleichzeitig nutzen

8 Drucken und Dokumentieren

- Tresore und Ordner drucken
- Dokumentation für Kunden

9 Konto

- E-Mail-Adresse ändern
- Master-Passwort ändern
- Angemeldete Geräte
- Feedback senden
- Konto löschen
- Protokoll
- Fehlerprotokoll

10 Fehler und Probleme

Ich kann mich nicht anmelden
Die App zeigt eine alte Version
Unterstützte Browser und Geräte
Kontakt bei Problemen

1 Erste Schritte

ERSTE SCHRITTE

Konto einrichten

Ein Keyfiler-Konto bekommst du über eine Einladung. Du erhältst einen Einladungslink, meist per E-Mail. Er gilt nur eine begrenzte Zeit und nur für ein einziges Konto.

Konto anlegen

1. Öffne den Einladungslink. Keyfiler öffnet dann den Assistenten `Konto anlegen` in zwei Schritten. Schließt du ihn, holst du ihn mit `Konto anlegen …` zurück.
2. **Schritt 1 – Über dich:** Gib deine `E-Mail-Adresse` ein – mit ihr meldest du dich künftig an – sowie `Vorname` und `Nachname`. So sehen alle, mit denen du teilst, wer du bist (siehe Dein Name). Klicke auf `Weiter`.
3. **Schritt 2 – Dein Master-Passwort:** Wähle ein `Master-Passwort` und wiederhole es. Es muss mindestens 12 Zeichen lang sein – besser 14 oder ein Satz aus mehreren Wörtern, den du dir gut merken kannst.
4. Klicke auf `Konto anlegen`. Dein Browser erzeugt jetzt deine Schlüssel. Das dauert einen Moment.
5. Keyfiler zeigt deinen Wiederherstellungsschlüssel. Speichere oder notiere ihn, bestätige mit `Ich habe den Schlüssel sicher aufbewahrt.` und klicke auf `Weiter`.

> **Das Master-Passwort ist der Schlüssel zu deinen Daten.** Es verlässt deinen Browser nie, und niemand kann es zurücksetzen – auch der Betreiber nicht. Vergisst du es, hilft nur noch der Wiederherstellungsschlüssel.

Die ersten Schritte

Nach der Anmeldung begrüßt dich Keyfiler mit einer kurzen Liste. Erledigte Schritte bekommen einen Haken.

- **Wiederherstellungsschlüssel aufbewahren:** Ist er beim Anlegen gespeichert, ist dieser Schritt schon erledigt.
- **Zwei-Faktor-Anmeldung einschalten:** Empfohlen. Zusätzlich zum Master-Passwort bestätigst du die Anmeldung dann mit einem Passkey (Fingerabdruck, Gesicht, PIN des Geräts) oder einem Code aus einer Authenticator-App – siehe Zwei-Faktor-Anmeldung einrichten.
- **Ersten Tresor anlegen:** Wähle eine der vier Kacheln. Mit `Leerer Tresor …` beginnst du leer. `Vorsorgeordner …` legt einen fertig gegliederten Vorsorgeordner an. `Beispieldaten` legt einen Beispiel-Tresor mit erfundenen Daten an, den du später wieder löschen kannst. `Importieren …` übernimmt Daten aus der Desktop-Version oder einem anderen Programm.

Testzugang

Wurdest du zu einem Testzugang eingeladen, steht die Laufzeit schon auf der Anmeldeseite. Einige Tage vor dem Ende erinnert dich ein Hinweis oben in der App. Danach ist keine Anmeldung mehr möglich, und 30 Tage nach dem Ende wird das Konto mit allen Daten gelöscht. Sichere deine Daten deshalb rechtzeitig mit einem Backup. Wenn du weitermachen möchtest, schreib uns an info@keyfiler.com.

Link abgelaufen oder schon benutzt? Bitte die Person, die dich eingeladen hat, um eine neue Einladung.

ERSTE SCHRITTE

Dein Name

Zu deinem Konto gehören dein Vor- und Nachname. Ihn sehen die Admins und alle, mit denen du Tresore teilst, die du als Vertrauensperson einlädst oder die dich eingeladen haben – statt nur deiner E-Mail-Adresse. In E-Mails von Keyfiler an diese Personen steht er zusammen mit deiner Adresse, z.B. „Anna Muster (anna@beispiel.de)“.

- Ändern kannst du ihn jederzeit unter Einstellungen › Konto › Name.
- Konten, die schon vor der Einführung bestanden, fragt Keyfiler nach der Anmeldung einmal danach. Mit Später geht es ohne weiter; bis dahin sehen andere deine E-Mail-Adresse.
- Anders als die Inhalte deiner Tresore liegt der Name unverschlüsselt auf dem Server – sonst könnten Admins und E-Mails ihn nicht anzeigen. Schreib deshalb nur deinen Namen hinein.

ERSTE SCHRITTE

Wiederherstellungsschlüssel

Keyfiler kennt dein Master-Passwort nicht – deshalb kann es niemand für dich zurücksetzen, auch der Betreiber nicht. Der Wiederherstellungsschlüssel ist dein Ersatzschlüssel: Mit ihm setzt du ein neues Master-Passwort, und alle deine Tresore bleiben erhalten.

> **Ohne Master-Passwort und ohne Wiederherstellungsschlüssel sind deine Daten verloren.** Auch wir können sie dann nicht wiederherstellen.

So sieht er aus

Der Schlüssel besteht aus 32 Zeichen in acht Vierergruppen, etwa XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX. Keyfiler zeigt ihn direkt nach dem Anlegen deines Kontos an. Du kannst ihn dort Kopieren oder Als Datei speichern und bestätigst mit Ich habe den Schlüssel sicher aufbewahrt.

So bewahrst du ihn richtig auf

- **Ausdrucken** und an einem sicheren Ort ablegen, zum Beispiel bei wichtigen Unterlagen. Am besten mit Notfallblatt drucken (siehe unten); die gespeicherte Textdatei eignet sich auch.
- **Getrennt vom Gerät:** Nicht auf dem Rechner oder Handy liegen lassen, mit dem du Keyfiler nutzt – und nicht unverschlüsselt in der Cloud oder per E-Mail.
- **Nicht in Keyfiler selbst:** Wenn du das Master-Passwort vergessen hast, kommst du an diesen Eintrag auch nicht heran.
- **Behandle ihn wie einen Hausschlüssel:** Wer ihn zusammen mit deinem Benutzernamen hat, kommt an deine Daten.

Das Notfallblatt

Das Notfallblatt fasst auf einer Seite zusammen, was du brauchst, um wieder in dein Konto zu kommen: Adresse der App, Benutzer, deine Anmeldewege, Wiederherstellungsschlüssel und -codes, deine Vertrauenspersonen und was im Notfall zu tun ist. Dein Master-Passwort druckt Keyfiler nie – dafür gibt es ein leeres Feld.

- **Jederzeit:** Einstellungen › Konto › Notfallblatt › Drucken …. Schlüssel und Codes trägst du von Hand ein – Keyfiler kennt sie nach dem Erzeugen selbst nicht mehr.
- **Beim Erzeugen:** Im Fenster mit dem neuen Wiederherstellungsschlüssel bzw. den neuen Codes gibt es Notfallblatt drucken. Dann stehen sie schon gedruckt darauf.

Erzeugst du später einen neuen Schlüssel oder neue Codes, gilt das alte Blatt nicht mehr: neu drucken, das alte vernichten. Wählst du beim Drucken „Als PDF speichern“, liegt der Schlüssel als Datei vor – dann auch die Datei sicher aufbewahren.

Einrichten oder neu erzeugen

1. Öffne die Einstellungen über deinen Namen unten links und wähle Konto.
2. Bei Wiederherstellungsschlüssel siehst du, ob er eingerichtet ist. Wähle Einrichten … bzw. Neu erzeugen …
3. Bestätige mit deinem Master-Passwort und klicke auf Erzeugen.
4. Bewahre den neuen Schlüssel auf. **Der bisherige ist damit ungültig.**

Einen neuen Schlüssel brauchst du, wenn du den alten verloren hast oder befürchtest, dass jemand anderes ihn kennt.

Master-Passwort vergessen?

1. Klicke auf der Anmeldeseite auf Master-Passwort vergessen?
2. Schritt **Schlüssel:** Gib deinen Benutzer und den Wiederherstellungsschlüssel ein und klicke auf Weiter. Ist die Zwei-Faktor-Anmeldung eingeschaltet, bestätigst du zusätzlich mit deinem Passkey (Mit Passkey bestätigen), einem Code aus der Authenticator-App oder einem Wiederherstellungscode.
3. Schritt **Neues Passwort:** Lege ein neues Master-Passwort fest – mindestens 12 Zeichen, besser 14 oder ein Satz aus mehreren Wörtern – und klicke auf Speichern und anmelden.

Deine anderen Geräte werden dabei abgemeldet. Dein Wiederherstellungsschlüssel bleibt gültig.

ERSTE SCHRITTE

Zwei-Faktor-Anmeldung einrichten

Mit der Zwei-Faktor-Anmeldung reicht das Master-Passwort allein nicht mehr: Nach dem Passwort bestätigst du die Anmeldung zusätzlich – mit einem **Passkey** oder mit einem sechsstelligen **Code aus einer Authenticator-App**. Wer nur dein Passwort kennt, kommt nicht hinein. Wir empfehlen sie ausdrücklich.

Beide Wege stehen gleichberechtigt nebeneinander: Du kannst nur Passkeys nutzen, nur die App oder beides. Die Verschlüsselung deiner Daten ändert sich dadurch nicht – sie hängt weiterhin nur am Master-Passwort.

Was ist ein Passkey?

Mit einem Passkey prüft dein Gerät, dass du es bist – so, wie du es auch entsperrst: per **Fingerabdruck** (Touch ID am Mac, Fingerabdruckleser unter Windows Hello, Android), per **Gesicht** (Face ID, Windows Hello mit Kamera) oder mit der **PIN des Geräts**. Auch ein **Sicherheitsschlüssel** wie ein YubiKey ist ein Passkey. An einem PC ohne Sensor kannst du dein Handy per QR-Code verwenden.

Fingerabdruck und Gesicht verlassen dein Gerät nie. Keyfiler bekommt nur eine signierte Bestätigung und speichert je Passkey einen öffentlichen Schlüssel, den Namen und die Zeitpunkte. Ein Passkey gilt nur für Keyfiler unter keyfiler.com.

Wo du sie einrichtest

Öffne die Einstellungen über deinen Namen unten links und wähle Konto. Im Block Zwei-Faktor-Anmeldung siehst du, ob sie eingeschaltet ist, und darunter je eine Zeile für Passkeys, Authenticator-App und Wiederherstellungscodes – jede mit ihrem eigenen Knopf. Direkt nach der Registrierung geht es auch über Einrichten … auf der Willkommensseite: Dort wählst du zuerst, ob du mit Passkey oder Authenticator-App beginnen möchtest.

Bevor du etwas änderst, bestätigst du – beim ersten Passkey bzw. der ersten App mit deinem Master-Passwort, danach mit Passkey, Code oder Wiederherstellungscode. Das gilt dann 5 Minuten, du musst also nicht für jeden Schritt neu bestätigen. Umbenennen geht ohne Bestätigung. So kann niemand, der kurz an deinen offenen Rechner kommt, einen eigenen zweiten Faktor eintragen oder deinen entfernen.

Nach 5 falschen Bestätigungen (Passwort, Code oder Passkey) meldet Keyfiler dich zur Sicherheit ab; die Versuche zählen auch in die Anmeldesperre.

Passkey hinzufügen

1. Klicke in der Zeile Passkeys auf Hinzufügen … – hast du schon welche, auf Verwalten … und dann Passkey hinzufügen … .
2. **Name:** Keyfiler schlägt Gerät und Browser vor, z.B. „Windows – Edge“. Gib ihm einen Namen, an dem du das Gerät später erkennst, etwa „Laptop“.
3. **Gerät:** Klicke auf Passkey erstellen . Dein Gerät öffnet ein eigenes Fenster – bestätige dort mit Fingerabdruck, Gesicht oder PIN, oder stecke deinen Sicherheitsschlüssel ein.
4. War es dein erster zweiter Faktor, zeigt Keyfiler jetzt zehn **Wiederherstellungscodes**. Speichere oder drucke sie und bestätige mit Ich habe sie gesichert . Sie werden nur dieses eine Mal angezeigt.

Synchronisiert oder nur auf einem Gerät?

Viele Passkeys liegen nicht nur auf dem Gerät, sondern in deinem Konto beim Anbieter – etwa im Google-Passwortmanager (Chrome, Android) oder im iCloud-Schlüsselbund (Apple). Dann sind sie auf all deinen Geräten mit demselben Konto da, und du brauchst dort keinen eigenen. Keyfiler zeigt dir das nach dem Einrichten und in der Liste: synchronisiert oder nur auf einem Gerät bzw. Schlüssel . Das meldet dein Gerät selbst; bei älteren Passkeys erscheint es nach der nächsten Anmeldung.

Synchronisiert ist bequem: Geht ein Gerät verloren, ist der Passkey nicht weg. Dafür hängt er an deinem Konto beim Anbieter. Ein zweiter, davon unabhängiger Weg – ein Passkey nur auf einem Gerät, ein Sicherheitsschlüssel oder die Authenticator-App – hilft, falls du dort einmal nicht hineinkommst.

> **Tipp:** Richte einen zweiten Passkey auf einem anderen Gerät ein, z.B. Handy und Laptop. Geht eines verloren, meldest du dich mit dem anderen an.

Unter Verwalten … benennst du einen Passkey mit dem Umbenennen-Symbol um, mit dem Papierkorb entfernst du ihn. Lösche ihn danach auch in der Passwort- bzw. Passkey-Verwaltung deines Geräts – dort bleibt er sonst als Eintrag stehen.

Authenticator-App einrichten

Du brauchst eine Authenticator-App auf dem Handy, zum Beispiel Google Authenticator, Microsoft Authenticator, 2FAS oder Aegis. Klicke in der Zeile Authenticator-App auf Einrichten … . Keyfiler führt dich in Schritten – oben siehst du, wo du bist:

1. **App:** Installiere eine Authenticator-App, falls noch nicht geschehen, und klicke auf Weiter .
2. **Verbinden:** Scanne den QR-Code mit der App. Bist du am Handy selbst, tippe auf in der Authenticator-App öffnen . Alternativ kannst du den angezeigten Schlüssel von Hand in die App eintragen.
3. **Bestätigen:** Tippe den Code, den die App jetzt anzeigt, in die sechs Kästchen. Nach der letzten Ziffer (oder mit Einschalten) ist die App eingerichtet.
4. **Codes sichern** bzw. **Fertig:** War die App dein erster zweiter Faktor, zeigt Keyfiler die zehn Wiederherstellungscodes. Hast du schon Passkeys, gelten deine bisherigen Codes weiter.

Anmelden mit zweitem Faktor

Nach dem Master-Passwort geht es so weiter:

- **Mit Passkey:** Hast du auf diesem Gerät schon einmal einen Passkey eingerichtet oder benutzt, fragt es gleich nach Fingerabdruck, Gesicht oder PIN. Erscheint das Fenster nicht von selbst, klicke auf Mit Passkey bestätigen . Auf einem anderen Gerät – etwa dem Handy, wenn dein Passkey nur auf dem PC liegt – fragt Keyfiler zuerst nach dem Code aus der App; Mit Passkey bestätigen steht dann darunter, z.B. für einen synchronisierten Passkey. Brichst du das Fenster ab oder findet das Gerät keinen Passkey, wechselt Keyfiler zum Code.
- **Mit Code:** Tippe den Code aus der Authenticator-App in die sechs Kästchen oder füge ihn aus der Zwischenablage ein (auch als „123 456“) – nach der letzten Ziffer geht es automatisch weiter. Hast du beides eingerichtet, wählst du

Code aus der Authenticator-App eingeben.

- **Ohne Passkey und App:** Wähle Wiederherstellungscode verwenden und gib einen deiner Wiederherstellungscodes ein. Jeder Code gilt genau einmal; Keyfiler sagt dir danach, wie viele noch übrig sind.

Wiederherstellungscodes erneuern oder Zwei-Faktor abschalten

In der Zeile Wiederherstellungscodes siehst du, wie viele unbenutzte Codes du noch hast; mit Neu erzeugen … bekommst du zehn neue, die alten werden ungültig. Die Authenticator-App entfernst du in ihrer Zeile mit Entfernen …. Abgeschaltet ist die Zwei-Faktor-Anmeldung, sobald weder ein Passkey noch die App eingerichtet ist – entfernst du also den letzten, fragt Keyfiler vorher nach und die Wiederherstellungscodes verfallen.

Neues Handy oder neues Gerät?

Übertrage den Eintrag „Keyfiler“ aus deiner Authenticator-App auf das neue Handy, *bevor* du das alte zurücksetzt oder abgibst. Die meisten Apps haben dafür eine Übertragungs- oder Sicherungsfunktion. Passkeys, die dein Gerät mit deinem Apple-, Google- oder Microsoft-Konto abgleicht, sind auf dem neuen Gerät meist schon da; sonst richtest du dort einen neuen Passkey ein und entfernst den alten in Keyfiler.

Handy oder Passkey verloren?

Melde dich mit einem anderen Passkey, der App oder einem Wiederherstellungscode an, entferne den verlorenen Passkey bzw. richte die App mit dem neuen Handy neu ein und erzeuge neue Wiederherstellungscodes. Hast du weder Passkey noch Handy noch Codes, schreib von der E-Mail-Adresse deines Kontos an info@keyfiler.com. Nach einer Rückfrage an diese Adresse setzen wir die Zwei-Faktor-Anmeldung zurück. Dein Master-Passwort brauchst du danach weiterhin – deine Inhalte bleiben verschlüsselt.

Tipp: Wird ein Code abgelehnt, obwohl er stimmt, geht meist die Uhr deines Handys falsch. Stelle Datum und Uhrzeit auf „automatisch“.

ERSTE SCHRITTE

Entsperren mit Passkey

Darf ein Passkey entsperren, meldest du dich mit ihm allein an – ohne Benutzer, ohne Master-Passwort und ohne Code. Dein Gerät fragt nach Fingerabdruck, Gesicht oder PIN, und Keyfiler ist offen. Fachlich ist das selbst schon eine Zwei-Faktor-Anmeldung: Du brauchst das Gerät *und* deinen Fingerabdruck bzw. die PIN.

Das ist eine bewusste Wahl je Passkey und standardmäßig aus. Master-Passwort und Wiederherstellungsschlüssel bleiben immer gültig.

Wie es funktioniert

Deine Daten öffnet ein Schlüssel, den nur du kennst – bisher kam er aus dem Master-Passwort. Viele Passkeys können zusätzlich ein Geheimnis liefern, das nur das Gerät kennt. Damit verschlüsselt dein Browser eine weitere Kopie deines Schlüssels. Der Server speichert nur diese verschlüsselte Kopie und kann sie nicht öffnen.

Einschalten

1. Öffne Einstellungen › Konto › Passkeys › Verwalten ….
2. Schalte beim gewünschten Passkey Zum Entsperren verwenden ein.
3. Lies den Hinweis. Bei einem **synchronisierten** Passkey bestätigst du ihn mit einem Häkchen (siehe unten).
4. Gib dein Master-Passwort ein – nur damit lässt sich dein Schlüssel für den Passkey verpacken – und klicke auf Einschalten.
5. Dein Gerät fragt einmal nach dem Passkey. Danach steht dort Darf entsperren.

Steht bei einem Passkey Kann nicht entsperren – nur als zweiter Faktor, hat dein Gerät beim Einschalten das nötige Geheimnis nicht geliefert. Das gilt für manche Passwortmanager und ältere Geräte; er bleibt trotzdem ein guter zweiter Faktor. Nach einem Update von Browser oder Betriebssystem kann es klappen – mit Erneut prüfen … versuchst du es noch einmal. Windows Hello kann es ab Windows 11 mit dem Update

vom Februar 2026. Ausschalten geht jederzeit mit demselben Schalter – die verschlüsselte Kopie wird dann gelöscht.

Anmelden und Entsperren

Auf der Anmeldeseite klickst du auf `Mit Passkey anmelden` und wählst im Fenster deines Geräts den Passkey. Hast du in diesem Browser schon einmal so entsperrt, steht nur noch dieser Knopf da; Benutzer und Master-Passwort öffnest du bei Bedarf mit `Weitere Anmeldeoptionen`. Brichst du die Passkey-Abfrage ab oder klappt sie nicht, erscheinen die Felder von selbst. Nach dem automatischen Sperren geht es genauso. Darf der gewählte Passkey nicht entsperren, meldest du dich wie gewohnt mit Master-Passwort und zweitem Schritt an.

Master-Passwort zwischendurch

Wer nur noch per Fingerabdruck entsperrt, vergisst leicht sein Master-Passwort. Deshalb fragt Keyfiler nach dem Entsperren mit Passkey alle 14 Tage einmal danach. Mit `Später` geht es trotzdem weiter; die Frage kommt beim nächsten Mal wieder. Unter `Einstellungen` › `Konto` › `Master-Passwort zwischendurch abfragen` stellst du alle 14 Tage, alle 30 Tage oder nie ein.

Worauf du achten solltest

- **Wer dein Gerät entsperren kann, kommt an deine Daten** – auch mit der Geräte-PIN. Schütze dein Gerät entsprechend.
- **Synchronisierte Passkeys** liegen in deinem Konto beim Anbieter (z.B. Google oder Apple) und sind auf all deinen Geräten mit diesem Konto. Wer dort hineinkommt und eines dieser Geräte entsperren kann, kommt dann auch an deine Keyfiler-Daten. Schütze das Konto beim Anbieter deshalb gut, z.B. mit Zwei-Faktor-Anmeldung.
- Der Betreiber kann das Entsperren mit Passkey für alle abschalten. Dann gelten deine Passkeys weiter als zweiter Faktor, und du meldest dich wieder mit dem Master-Passwort an.

ERSTE SCHRITTE · KEYFILER ALS APP INSTALLIEREN

Keyfiler als App installieren

Keyfiler läuft im Browser – du kannst es aber auch wie eine gewöhnliche App installieren. Dann bekommt Keyfiler ein eigenes Symbol im Startmenü, im Dock oder auf dem Home-Bildschirm und öffnet sich in einem eigenen Fenster ohne Adressleiste und Tabs.

Was sich ändert – und was nicht

- **Eigenes Fenster:** Keyfiler startet wie ein Programm und geht nicht zwischen vielen Browser-Tabs verloren.
- **Immer aktuell:** Die installierte App prüft bei jedem Start, ob es eine neue Version gibt, und lädt sie dann. Ein Update-Download ist nicht nötig.
- **Gleiche Sicherheit:** Es ist dieselbe Keyfiler-Anwendung. Du meldest dich wie gewohnt mit Master-Passwort und ggf. zweitem Faktor an, verschlüsselt wird weiterhin in deinem Browser.
- **Kein App-Store:** Keyfiler gibt es nicht in App Store oder Google Play. Installiert wird ausschließlich über deinen Browser von `keyfiler.com/app`.

> **Achte auf die Adresse.** Installiere Keyfiler nur, wenn in der Adressleiste `https://keyfiler.com/app` steht. Eine App mit ähnlichem Namen aus einem App-Store oder von einer anderen Adresse stammt nicht von uns.

Wähle dein Gerät

Chrome oder Edge
Windows, Mac, Linux

Safari
Mac

Firefox
Windows, Mac, Linux

Android
Handy und Tablet

iPhone & iPad
Safari und andere Browser

Gemeinsam genutzte Computer: Installiere Keyfiler nur auf Geräten, die du allein nutzt. Auf fremden oder öffentlichen Rechnern meldest du dich besser im Browser an – am besten in einem privaten Fenster – und meldest dich danach wieder ab.

KEYFILER ALS APP INSTALLIEREN

Windows, Mac & Linux: Chrome und Edge

Google Chrome

1. Öffne `keyfiler.com/app` in Chrome.
2. Klicke rechts in der Adressleiste auf das Symbol `App installieren` (ein Bildschirm mit Pfeil nach unten).
   Ist das Symbol nicht zu sehen: Öffne das Menü `⋮` oben rechts und wähle `Streamen, speichern und teilen` › `Seite als App installieren …`
3. Bestätige mit `Installieren`.

Microsoft Edge

1. Öffne `keyfiler.com/app` in Edge.
2. Klicke rechts in der Adressleiste auf das Symbol `App verfügbar` oder öffne das Menü `…` und wähle `Apps` ›
   `Diese Website als App installieren`.
3. Bestätige mit `Installieren`.

Keyfiler starten

- **Windows:** Keyfiler steht im Startmenü. Mit einem Rechtsklick auf das Symbol kannst du es an die Taskleiste anheften.
- **Mac:** Keyfiler liegt im Ordner `Programme` (bei Chrome im Unterordner `Chrome-Apps`) und lässt sich über Spotlight oder das Dock starten.
- **Linux:** Keyfiler erscheint im Anwendungsmenü deiner Arbeitsumgebung.

Die Bezeichnungen der Menüpunkte können sich je nach Browser-Version leicht unterscheiden.

KEYFILER ALS APP INSTALLIEREN

Mac: Safari

Ab macOS Sonoma (14) kann Safari Websites als App ins Dock legen.

1. Öffne `keyfiler.com/app` in Safari.
2. Wähle in der Menüleiste `Ablage` › `Zum Dock hinzufügen …`
   Alternativ: Klicke auf das Teilen-Symbol in der Symbolleiste und wähle `Zum Dock hinzufügen`.
3. Prüfe den Namen und klicke auf `Hinzufügen`.

Keyfiler erscheint im Dock und wird im Ordner `Programme` deines Benutzerordners abgelegt. Du findest es auch über Spotlight.

Ältere macOS-Versionen bieten diese Funktion nicht. Nutze dort Chrome oder Edge oder lege ein Lesezeichen an.

KEYFILER ALS APP INSTALLIEREN

Firefox

Windows

Neuere Firefox-Versionen können Websites als Web-App an die Taskleiste anheften.

1. Öffne `keyfiler.com/app` in Firefox.
2. Klicke rechts in der Adressleiste auf das Symbol `Zur Taskleiste hinzufügen`.
3. Bestätige die Rückfrage. Keyfiler erscheint in der Taskleiste und öffnet sich künftig in einem eigenen, schlichten Fenster.

Fehlt das Symbol, ist die Funktion in deiner Firefox-Version noch nicht verfügbar oder nicht aktiviert. Bei Firefox aus dem Microsoft Store gibt es sie nicht.

Mac und Linux

Auf Mac und Linux kann Firefox Websites bisher nicht als App installieren. Du hast zwei Möglichkeiten:

- Lege ein Lesezeichen für `keyfiler.com/app` in der Lesezeichen-Symbolleiste an.
- Installiere Keyfiler über Chrome oder Edge bzw. auf dem Mac über Safari.

Android

Öffne `keyfiler.com/app`, tippe auf das Menü `⋮` und wähle `Zum Startbildschirm hinzufügen`.

KEYFILER ALS APP INSTALLIEREN

Android

Chrome

1. Öffne `keyfiler.com/app` in Chrome.
2. Tippe oben rechts auf das Menü `⋮`.
3. Wähle `App installieren` oder – je nach Version – `Zum Startbildschirm hinzufügen` › `Installieren`.
4. Bestätige. Keyfiler erscheint auf dem Startbildschirm und in der App-Übersicht.

Andere Browser

Auch Samsung Internet, Edge und Firefox bieten im Menü eine Option wie `Zum Startbildschirm hinzufügen` oder `Seite hinzufügen zu` › `Startbildschirm`.

Erscheint Keyfiler nach der Installation nicht auf dem Startbildschirm, findest du es in der App-Übersicht und kannst es von dort auf den Startbildschirm ziehen.

KEYFILER ALS APP INSTALLIEREN

iPhone & iPad

Safari

1. Öffne `keyfiler.com/app` in Safari.
2. Tippe auf das Teilen-Symbol (Quadrat mit Pfeil nach oben). Ab iOS 26 erreichst du es über die Taste `…` neben der Adressleiste.

3. Wähle Zum Home-Bildschirm. Falls der Eintrag fehlt, scrolle in der Liste nach unten oder tippe auf Mehr.
4. Achte darauf, dass Als Web-App öffnen eingeschaltet ist (ab iOS 26), und tippe auf Hinzufügen.

Keyfiler liegt jetzt als Symbol auf dem Home-Bildschirm und öffnet sich ohne Safari-Leisten im Vollbild.

Chrome, Edge und Firefox

Ab iOS 16.4 geht das auch in anderen Browsern: Tippe auf das Teilen-Symbol (bei Chrome rechts in der Adressleiste) und wähle Zum Home-Bildschirm.

> Die genaue Lage der Schaltflächen hängt von der iOS-Version und den Safari-Einstellungen ab.

KEYFILER ALS APP INSTALLIEREN

App wieder entfernen

Beim Entfernen der App bleiben deine Tresore unberührt – sie liegen verschlüsselt auf dem Server, nicht in der App. Du kannst dich jederzeit wieder im Browser anmelden.

- **Chrome und Edge:** Öffne die Keyfiler-App, klicke oben rechts auf das Menü ⋮ bzw. … und wähle Keyfiler deinstallieren. Unter Windows geht es auch per Rechtsklick auf das Symbol im Startmenü › Deinstallieren.
- **Safari auf dem Mac:** Öffne im Finder deinen Benutzerordner › Programme und ziehe Keyfiler in den Papierkorb.
- **Firefox unter Windows:** Rechtsklick auf das Symbol in der Taskleiste › Von Taskleiste lösen.
- **Android:** Halte das Keyfiler-Symbol gedrückt und wähle Deinstallieren bzw. Entfernen.
- **iPhone & iPad:** Halte das Symbol gedrückt, tippe auf App entfernen › Vom Home-Bildschirm entfernen.

2 Tresore und Ordner

TRESORE UND ORDNER

Tresore anlegen und Kategorien

Ein Tresor ist eine Sammlung zusammengehöriger Daten, zum Beispiel „Privat“, „Firma“ oder je ein Tresor pro Kunde. Jeder Tresor hat einen eigenen Schlüssel. Kategorien gruppieren deine Tresore in der Seitenleiste.

Neuen Tresor anlegen

1. Klicke in der Seitenleiste auf das `+` neben `Tresore` und wähle `Neuer Tresor` (Tastatur: `Einfg` in der Seitenleiste).
2. Gib einen Namen ein, wähle eine Kategorie und klicke auf `Anlegen`.

Im selben Menü findest du `Aus anderem Programm importieren …` (auch für Keyfiler für Windows) und `Aus Sicherung wiederherstellen …`

Tresor bearbeiten oder löschen

Über das Menü `⋯` am Tresor (oder `F2`) änderst du Name und Kategorie. Zum Löschen musst du den Namen des Tresors zur Bestätigung eintippen.

> **Ein gelöschter Tresor landet nicht im Papierkorb.** Er ist mit allen Ordnern, Dokumenten und Anhängen endgültig weg. Erstelle vorher eine Sicherung, wenn du dir nicht ganz sicher bist.

Kategorien

- **Neue Kategorie:** Wähle beim Anlegen oder Bearbeiten eines Tresors im Feld `Kategorie` den Eintrag `Neue Kategorie …`
- **Tresor umsortieren:** Ziehe einen Tresor in der Seitenleiste einfach auf eine andere Kategorie.
- **Reihenfolge, Namen, Löschen:** `Einstellungen` › `Kategorien` › `Kategorien verwalten …` Die Reihenfolge dort ist die Reihenfolge in der Seitenleiste; Tresore ohne Kategorie stehen immer am Ende.

TRESORE UND ORDNER

Tresore mit anderen teilen

Einen Tresor kannst du mit anderen Keyfiler-Nutzern gemeinsam verwenden – etwa „Familie“ mit deinem Partner oder die Unterlagen eines Kunden mit einem Kollegen. Jeder meldet sich mit seinem eigenen Konto und Master-Passwort an. Teilen kann jeder mit Vollzugang (also nicht mit einem Testzugang oder einem Konto nur als Vertrauensperson), und zwar die eigenen Tresore.

Person einladen

1. Klick am Tresor auf `⋯` (oder rechte Maustaste) und wähle `Teilen …`
2. Wähle `Person einladen …`, gib an, für wen der Link ist (nur für dich sichtbar), und was die Person darf.
3. Unter `Zugriff` legst du fest, wie lange die Person den Tresor sehen darf: `Unbefristet`, 7 oder 30 Tage, 90 Tage, ein Jahr oder `Bis zu einem Tag …` – etwa für einen Handwerker oder eine Urlaubsvertretung. Danach endet der Zugriff von selbst.
4. Ob die Person schon ein Keyfiler-Konto hat, musst du nicht wissen: Der Link funktioniert wie beim Notfallzugang mit und ohne Konto. Wer schon eins hat, meldet sich an; wer noch keins hat, legt damit eins an – als Testzugang für 30 Tage, den der Admin in einen Vollzugang umwandeln kann.

5 Link erzeugen, dann Link kopieren oder Mit eigenem E-Mail-Programm … und den Link an die Person schicken. Von Keyfiler selbst verschicken lässt sich diese Einladung nicht: Im Link steckt der Schlüssel zum Tresor, den auch der Server nie sehen soll.

> **Der Link ist der Schlüssel.** Er öffnet den Tresor, gilt einmal und 7 Tage lang. Keyfiler zeigt ihn nur beim Erzeugen – der Schlüssel darin steht hinter dem „#“ und gelangt nie zum Server. Schick ihn nur an die Person, für die er gedacht ist. Geht er verloren, zieh die Einladung unter Offene Einladungen zurück und erzeuge eine neue.

Was die anderen dürfen

- **Lesen:** alles ansehen und kopieren, auch Anhänge ansehen und herunterladen, drucken und sichern – aber nichts ändern. Statt Bearbeiten steht oben am Dokument Nur lesen; Einträge lassen sich mit Kopieren nach … in einen eigenen Tresor übernehmen.
- **Bearbeiten:** zusätzlich Dokumente, Ordner und Anhänge anlegen, ändern, verschieben und in den Papierkorb legen.
- **Nur du als Besitzer** kannst den Tresor umbenennen, löschen, weiter teilen und Rollen ändern. Anhänge zählen bei deinem Speicherplatz.

Einladung annehmen

Wer den Link öffnet, meldet sich an (oder legt sein Konto an). Danach erscheint Einladung zu einem gemeinsamen Tresor mit Name, Besitzer und Rolle – Annehmen, und der Tresor steht in der Seitenleiste. Geteilte Tresore tragen dort am rechten Rand das Teilen-Symbol (drei verbundene Punkte) – bei allen Beteiligten, auch beim Besitzer. Mit Später schließt du den Dialog, ohne dich festzulegen – Keyfiler merkt sich den Link aber nicht: Um doch anzunehmen, öffne ihn noch einmal aus deiner Nachricht, solange er gilt. Ablehnen macht den Link sofort ungültig, und der Besitzer erfährt es. Die Kategorie wählt jeder für sich; den Namen legt der Besitzer fest.

Zugriff ändern, entziehen, verlassen

- **Befristen:** Mit dem Kalender-Symbol in der Zeile legst du fest, bis zu welchem Tag eine Person Zugriff hat, oder machst ihn wieder unbefristet. Nach dem letzten Tag sieht sie den Tresor nicht mehr – wie beim Entziehen, nur von selbst –, und du bekommst oben in der App einen Hinweis. Mit Neu verschlüsseln … darin bekommt der Tresor gleich einen neuen Schlüssel – wie beim Entziehen. Der Notfallzugang hat bewusst kein Ablaufdatum.
- Unter Teilen … änderst du die Rolle oder entziehst mit dem × den Zugriff. Was die Person schon gesehen oder heruntergeladen hat, lässt sich nicht zurückholen – ändere wichtige Kennwörter, wenn nötig.
- Beim Entziehen ist Tresor neu verschlüsseln vorausgewählt: Keyfiler verschlüsselt dann in deinem Browser alles im Tresor mit einem neuen Schlüssel. Ein Schlüssel, den sich die Person früher gemerkt hat, passt danach zu nichts mehr, was auf dem Server liegt. Das dauert bei vielen Anhängen etwas; bricht es ab, bleibt der Tresor unverändert lesbar und du kannst es noch einmal versuchen. Offene Einladungen werden dabei zurückgezogen.
- Die übrigen Mitglieder merken davon nichts: Keyfiler verschlüsselt den neuen Schlüssel für jedes von ihnen mit dessen persönlichem Schlüsselpaar, sodass nur diese Person ihn öffnen kann – mit dem alten Tresorschlüssel kommt man nicht heran. Ihr Keyfiler übernimmt ihn beim nächsten Laden von selbst; hat jemand den Tresor gerade offen, lädt er ihn kurz neu.
- Hat sich ein Mitglied seit der Einführung der Schlüsselpaare noch nie angemeldet, sagt Keyfiler beim Neuverschlüsseln Bescheid: Die Person muss sich zuerst einmal anmelden, dann klappt es.
- Als Mitglied siehst du unter ⋯ → Wer hat Zugriff? alle Beteiligten – und, wenn dein Zugriff befristet ist, bis wann er gilt – und verlässt den Tresor mit Tresor verlassen …

Schlüssel-Fingerabdruck

In Wer hat Zugriff? steht bei jeder Person der Anfang ihres Schlüssel-Fingerabdrucks, etwa Schlüssel 6C9F 1632 1A78 B3C3 (beim Darüberfahren vollständig). Deinen eigenen findest du unter Einstellungen › Konto. Vergleicht ihr ihn – am Telefon oder persönlich – und er stimmt überein, ist sicher, dass der Server keinen fremden Schlüssel untergeschoben hat. Nötig ist das nicht; es ist eine zusätzliche Prüfung für besonders Vorsichtige.

Überblick: Einstellungen › Gemeinsame Tresore

Unter Einstellungen › Gemeinsame Tresore siehst du alles, was dich betrifft – und nur das, auch als Admin:

- **Von mir geteilt:** deine geteilten Tresore mit Anzahl der Mitglieder, offenen Einladungen, Dokumenten und Speicher. Ein Klick klappt einen Tresor auf: Mitglieder mit Rolle, Beginn und „Zugriff bis“, offene Einladungen. Teilen … in der Zeile öffnet die Verwaltung.
- **Neuer Schlüssel ausstehend:** Nach dem Neuverschlüsseln zeigt ein roter Hinweis, wer den neuen Schlüssel noch nicht übernommen hat. Er verschwindet, sobald sich die Person einmal angemeldet hat.
- **Mit mir geteilt:** Tresore anderer, in denen du Mitglied bist – mit Besitzer, Rolle und, falls befristet, bis wann. Wer hat Zugriff? … zeigt alle Beteiligten.
- **Verlauf meiner Tresore:** für die letzten 90 Tage, wer einem deiner Tresore beigetreten ist, eine Einladung abgelehnt, ihn verlassen hat, entfernt wurde, wessen befristeter Zugriff abgelaufen ist oder wer sein Konto gelöscht hat. Einzelne Einträge entfernst du mit Löschen. Bei solchen Ereignissen erscheint außerdem oben in der App ein Hinweis – auch, wenn jemand deine Einladung angenommen hat; Verlauf führt hierher, Ausblenden markiert ihn als gelesen. Das Symbol geteilt neben dem Tresor in der Seitenleiste erscheint, sobald jemand angenommen hat, und verschwindet, wenn niemand mehr Zugriff hat – ohne neue Anmeldung, spätestens nach etwa einer halben Minute.

Eine Übersicht über die gemeinsamen Tresore anderer Konten gibt es bewusst nicht, auch nicht für Admins. Beitritt, Entzug und Ablauf stehen nur als Nachweis im Protokoll.

TEILEN

Teilen per Link

Mit einem Link gibst du eine Kopie eines einzelnen Dokuments an jemanden weiter, der kein Keyfiler-Konto hat – zum Beispiel die WLAN-Zugangsdaten an Gäste oder Kontodaten an den Steuerberater. Die Kopie ist eine Momentaufnahme: Änderungen, die du danach am Dokument machst, sieht der Empfänger nicht.

1. Öffne das Dokument und wähle oben Teilen per Link oder ⋯ › Teilen per Link …
2. **Inhalt:** Wähle die Zeilen aus, die in die Kopie sollen – eine PIN lässt du z.B. einfach weg. Überschriften kommen automatisch mit, sobald eine Zeile darunter gewählt ist. Bemerkungen und Anhänge (zusammen höchstens 10 MB) gibst du auf Wunsch mit.
3. **Schutz:** Lege fest, wie lange der Link gilt (1 Stunde bis 30 Tage) und wie oft er sich öffnen lässt: Einmal öffnen, dann löschen, 5-mal oder unbegrenzt. Mit Nur für eine bestimmte E-Mail-Adresse gilt der Link nur für die Person mit dieser Adresse (siehe unten). Mit Zusätzlich mit Passwort schützen braucht der Empfänger außerdem ein Passwort, das du ihm getrennt gibst, am besten am Telefon. Beides lässt sich kombinieren.
4. Kopiere den Link, schick ihn per E-Mail oder zeig ihn mit QR-Code als Code, den dein Gegenüber mit der Handykamera scannt.

- **Sicher:** Dein Browser verschlüsselt die Kopie. Der Schlüssel steht nur im Link hinter dem „#“ – diesen Teil schicken Browser nie an den Server. Weder der Server noch der Betreiber können die Kopie lesen, nur wer den Link hat (und ggf. das Passwort).
- **Für den Empfänger:** Er öffnet den Link im Browser, ohne Konto und ohne Cookie, und sieht die Kopie nur zum Lesen – mit Kopieren und Aufdecken wie in Keyfiler. Erst Dokument öffnen zählt als Abruf; ein falsch getipptes Passwort verbraucht keinen. Anhänge lassen sich nach dem Öffnen 30 Minuten laden.
- **Nur für eine bestimmte E-Mail-Adresse:** Der Empfänger gibt beim Öffnen seine Adresse ein und bekommt einen 6-stelligen Code per E-Mail, der 10 Minuten gilt. Die E-Mail nennt dich als Absender und enthält bewusst keinen Link. Ein weitergeleiteter Link nützt so allein nichts. Andere Adressen bekommen keine E-Mail, und die Seite verrät nicht, ob eine Adresse stimmt. Nach 5 falschen Codes ist der Link gesperrt und gelöscht; höchstens 5 Code-E-Mails je Link. Keyfiler speichert die Adresse nicht, nur einen Prüfwert – frag den Empfänger vorher, ob er mit der E-Mail einverstanden ist.
- **QR-Code:** Praktisch, wenn du jemandem gegenübersitzt – etwa Gästen das WLAN. Der Code enthält den ganzen Link samt Schlüssel; Keyfiler erzeugt ihn nur in deinem Browser. Wer ihn abfotografiert, hat den Link – behandle ihn also genauso vertraulich. Mit

Als Bild speichern bekommst du ihn als PNG, etwa zum Ausdrucken. In die E-Mail kommt der Code nicht: Wer die E-Mail hat, klickt einfach auf den Link.

- **Einmal öffnen, dann löschen:** Nach dem ersten Öffnen ist der Link verbraucht; Anhänge lassen sich noch 30 Minuten laden, danach löscht Keyfiler die Kopie samt Anhängen endgültig.
- **Überblick:** Im Dokument steht „1 aktiver Link". Unter Einstellungen › Geteilte Links siehst du alle gültigen Links mit Ablauf und Abrufen; dort kopierst du einen Link erneut, zeigst ihn als QR-Code oder widerrufst ihn – die Kopie ist dann sofort gelöscht. Abgelaufene und aufgebrauchte Links löscht Keyfiler von selbst.
- **Grenzen:** Höchstens 20 gültige Links gleichzeitig. Mit „Nur lesen" in einem gemeinsamen Tresor und beim Notfallzugang lassen sich keine Links erstellen. Admins können die Funktion unter Administration › System für alle abschalten.
- Gib den Link nur an die Person weiter, für die er gedacht ist: Wer ihn hat, kann die Kopie lesen.

TRESORE UND ORDNER

Ordner anlegen und sortieren

Innerhalb eines Tresors ordnest du deine Dokumente in Ordnern und Unterordnern – so tief verschachtelt, wie du möchtest.

Ordner und Dokumente anlegen

Öffne das Menü ⋯ eines Tresors oder Ordners (oder klicke mit der rechten Maustaste) und wähle Neuer Ordner bzw. Neues Dokument. In der Liste geht es auch per Tastatur: Einfg legt ein Dokument an, Strg + Einfg einen Ordner.

Verschieben und kopieren

- **Ziehen und ablegen:** Ziehe Ordner oder Dokumente an die neue Stelle. Hältst du beim Ablegen Strg (Mac: Alt), wird kopiert statt verschoben.
- **In einen anderen Tresor:** Ziehe die Einträge auf den Ziel-Tresor oder nutze im Menü Verschieben nach … bzw. Kopieren nach …
- **Mehrere auf einmal:** Mit Strg + Klick markierst du einzelne Einträge, mit Umschalt + Klick einen Bereich, mit Strg + A alle. Ein markierter Ordner nimmt seinen ganzen Inhalt mit: Was darin liegt, zeigt ein blasses Häkchen und lässt sich nicht noch einmal einzeln markieren; vorher einzeln markierte Einträge darin werden abgewählt.
- **Vertan?** Nach dem Verschieben, Kopieren oder Löschen erscheint kurz eine Meldung mit Rückgängig (oder Strg + Z).

Weitere Aktionen im Menü

Umbenennen (F2), Duplizieren, Drucken …, Als Vorlage speichern (bei Dokumenten) und In den Papierkorb (Entf).

Schnell wieder heraus

Der Pfad über der Liste und der Pfad über dem Titel eines Dokuments (z.B. Privat / Bank) lassen sich anklicken – so springst du direkt in einen übergeordneten Ordner. Am Handy führt das Haus neben dem Zurück-Pfeil im Dokument bzw. Start in der Leiste unten aus jeder Tiefe zur Übersicht mit Favoriten und Tresoren. Neu in der Leiste legt in der Übersicht einen Tresor an, in einem Tresor ein Dokument oder einen Ordner.

Am Handy geht es Ebene für Ebene: Die Übersicht zeigt Kategorien und Tresore, ein Tipp auf einen Tresor (Pfeil ›) öffnet seine Ordner und Dokumente, ein Tipp auf einen Ordner den nächsten. Mit dem Zurück-Pfeil geht es eine Ebene hoch. Den aufklappbaren Ordnerbaum gibt es am Rechner und Tablet. Nach dem nächsten Anmelden landest du am Handy wieder dort, wo du zuletzt warst – in der Übersicht, in der Liste oder im Dokument.

TRESORE UND ORDNER

Papierkorb

Gelöschte Ordner und Dokumente landen zunächst im Papierkorb. Von dort kannst du sie zurückholen, bis du sie endgültig löschst.

In einem gemeinsamen Tresor sehen den Papierkorb nur du als Besitzer und wer Bearbeiten darf. Wer nur Lesen darf – und auch eine Vertrauensperson im Notfallzugang – bekommt Gelöschtes gar nicht erst zu sehen. Was du in deinem Vorsorgeordner verwirfst, bleibt also bei dir.

1. Klicke unten in der Seitenleiste auf Papierkorb (am Handy: Start, dann unten in der Übersicht).
2. Du siehst jeden Eintrag mit Herkunft, Gelöscht am und Inhalt.
3. Hole einen Eintrag an seinen alten Platz zurück oder lösche ihn Endgültig. Mit Papierkorb leeren löschst du alles auf einmal.

> **Endgültig gelöschte Einträge lassen sich nicht zurückholen** – außer aus einer Sicherung, die den Papierkorb übrigens mit sichert.

Ganze **Tresore** gehen beim Löschen nicht in den Papierkorb, sondern sind sofort weg.

3 Vorsorge

VORSORGE

Vorsorgeordner

Ein Vorsorgeordner sammelt alles, was deine Angehörigen im Ernstfall brauchen: Vollmachten, Konten, Versicherungen, Verträge, Ärzte, digitaler Nachlass und deine Wünsche. Er ist ein ganz normaler Tresor, nur schon fertig gegliedert – du musst nur noch ausfüllen.

Vorsorgeordner anlegen

1. Klicke in der Seitenleiste bei Tresore auf + und wähle Neuer Vorsorgeordner … (oder Strg + K › Neuer Vorsorgeordner).
2. Trag ein, für wen der Ordner ist, etwa deinen Namen oder „Mama“. Daraus ergibt sich ein Vorschlag für den Namen. Mit Mit Beispieldaten füllen sind die Dokumente teilweise mit erfundenen Angaben gefüllt – zum Ausprobieren.
3. Mit Anlegen entstehen 13 Bereiche mit 63 vorbereiteten Dokumenten in der Kategorie Vorsorge, dazu ganz oben die Nachricht an meine Vertrauensperson(en).

Alles darin ist freiwillig: Fülle aus, was auf dich zutrifft und was du gerade weißt. Ein unvollständiger Ordner hilft deinen Angehörigen mehr als gar keiner – jede Angabe ist im Notfall wertvoll.

Du kannst mehrere Vorsorgeordner anlegen, zum Beispiel einen für dich und einen für deine Eltern, deren Angelegenheiten du regelst. In der Seitenleiste tragen Vorsorgeordner am rechten Rand das Notfall-Symbol (ein Herz mit Pulslinie) – genau wie die Vorsorgeordner anderer, auf die du über einen Notfallzugang zugreifen kannst.

Alles rund um deine Vorsorgeordner findest du auch gesammelt unter Einstellungen › Vorsorge: anlegen, Übersicht öffnen, Notfallzugang verwalten und fehlende Bereiche wieder hinzufügen.

Ausfüllen

Die vorbereiteten Dokumente haben schon alle Zeilen. Leere Zeilen zeigen blass einen Hinweis, was hineingehört – etwa bei Vollmachten Original liegt mit „z.B. Ordner im Arbeitszimmer, beim Notar“. Ein Klick auf eine leere Zeile öffnet das Bearbeiten genau dort. Scans wie den Personalausweis oder die Vollmacht legst du als Anhang dazu.

Weitere Versicherungen, Verträge oder Online-Konten legst du mit den Vorsorge-Vorlagen an, die beim Anlegen eines Dokuments zur Auswahl stehen.

Übersicht: Was fehlt noch?

Öffnest du den Vorsorgeordner, zeigt Keyfiler rechts die Übersicht – sie ist die Startseite des Vorsorgeordners; in der Liste stehen nur die Bereiche. Von überall im Vorsorgeordner kommst du über Übersicht im Pfad über dem Titel jedes Dokuments zur Übersicht zurück, am Handy ebenso. Dort siehst du, wie viele Dokumente insgesamt und je Bereich ausgefüllt sind – auch selbst angelegte Dokumente und Bereiche zählen mit. Ein Klick auf einen Bereich öffnet sein erstes noch offenes Dokument. In der Liste zeigt ein Punkt hinter dem Namen den Stand wie eine Ampel: grau = offen, ocker = teilweise, grün = vollständig. Fährst du mit der Maus darüber, siehst du, wie viele Felder schon ausgefüllt sind.

Vollständig ist ein Dokument, wenn jede Zeile einen Inhalt hat; Ankreuzen-Zeilen zählen dabei nicht mit, Ja/Nein-Fragen müssen beantwortet sein. In der Übersicht zählt ein Dokument schon als ausgefüllt, sobald es teilweise ausgefüllt ist. Ja/Nein-Fragen und Ankreuzen-Zeilen beantwortest du direkt in der Ansicht, ohne Bearbeiten. Mit Als durchgesehen markieren hältst du fest, wann du den Ordner zuletzt geprüft hast. Bei jedem Bereich steht außerdem, wann darin zuletzt etwas geändert wurde – so siehst du, was angestaubt ist.

Liegt die letzte Durchsicht länger als ein Jahr zurück, erinnert dich ein Hinweis oben in der App daran, mit Übersicht kommst du direkt hin; Später blendet ihn für eine Woche aus. Den Abstand (6, 12 oder 24 Monate oder nie) stellst du unter Einstellungen › Vorsorge › An Durchsicht erinnern ein.

Nachricht an deine Vertrauenspersonen

Ganz oben in der Übersicht steht als Kachel die Nachricht (lässt du sie leer, sehen deine Vertrauenspersonen sie gar nicht) – sie heißt Nachricht von und dein Name (bzw. der Name, für den der Vorsorgeordner angelegt ist), für dich wie für deine Vertrauenspersonen – mit dem Anfang des Textes; ein Klick öffnet sie, ist sie noch leer, gleich zum Schreiben. In der Liste steht sie nicht – die Suche findet sie aber wie jedes Dokument. Hier schreibst du, was deine Vertrauenspersonen im Ernstfall als Erstes wissen sollen – was jetzt zu tun ist, ein Dank, ein Abschied, ganz wie du möchtest. Es ist freiwillig und zählt in der Übersicht nicht mit; drucken kannst du es wie jedes Dokument.

Öffnet eine Vertrauensperson den Vorsorgeordner über den Notfallzugang und steht in der Nachricht etwas, weist Keyfiler sie zuerst in einem Fenster darauf hin; mit Nachricht lesen öffnet sie die Nachricht. Hast du das Dokument gelöscht, holst du es in der Übersicht unter Nicht in diesem Vorsorgeordner zurück.

Fragebogen zum Ausdrucken

Oft legen Kinder den Vorsorgeordner für ihre Eltern an – und nicht jeder mag oder kann dafür am Computer sitzen. In der Übersicht unter den Bereichen druckst du mit Fragebogen drucken … einen Fragebogen, mit dem ihr den Ordner gemeinsam ausfüllt, wie ein Gespräch am Küchentisch. Die erste Seite erklärt, wie ihr vorgeht; danach kommt je Bereich eine Seite mit den Fragen, den grauen Hinweisen, Kästen zum Schreiben und einem Kästchen Trifft nicht zu.

- Auswahl – wie beim Drucken: alle Bereiche zum Ankreuzen, die noch nicht vollständigen Dokumente sind vorausgewählt. Nur unvollständige und Alle auswählen setzen die Auswahl auf einen Klick. Was als „Trifft nicht zu“ markiert ist, steht nicht zur Auswahl.
- Inhalt – leere Felder zum Ausfüllen oder die bisherigen Angaben eingetragen, zum Prüfen und Ergänzen. Kennwörter, PINs und andere verdeckte Zeilen druckt Keyfiler nie; ihr Kasten bleibt leer, und an der Bezeichnung steht der Hinweis, sie besser direkt in Keyfiler einzutragen.
- Selbst angelegte Dokumente und Bereiche kommen mit, die Dokumente eines Bereichs in der Reihenfolge der Liste. Liegt ein Dokument in einem Unterordner, steht dieser davor, etwa „Auto › Haftpflicht“.

Reihenfolge der Bereiche

Die Bereiche stehen zunächst in einer vorgeschlagenen Reihenfolge – von Persönliches bis Letzte Wünsche. Mit Reihenfolge ändern unter den Bereichen in der Übersicht bringst du sie in die Reihenfolge, die für dich passt: Jeder Bereich bekommt links einen Griff ⋮⋮ – fass ihn an und zieh den Bereich an eine andere Stelle, mit der Maus oder mit dem Finger. Eine rote Linie zeigt, wo er landet. Mehrere auf einmal verschiebst du wie die Zeilen eines Dokuments: Ein Klick auf den Griff wählt einen Bereich aus (mit Umschalt alle bis dorthin), dann ziehst du einen der ausgewählten. Mit der Tastatur steuerst du den Griff mit Tab an, wählst mit der Leertaste aus und verschiebst mit Alt + ↑ / ↓. Fertig speichert, Abbrechen lässt alles, wie es war. Sie gilt im ganzen Vorsorgeordner: in der Übersicht, in Seitenleiste und Liste und im Fragebogen. Einen selbst angelegten Bereich (Ordner auf oberster Ebene) stellt Keyfiler zunächst ans Ende – schieb ihn dorthin, wo er hingehört.

In der Übersicht und im Fragebogen tragen die Bereiche Nummern in dieser Reihenfolge, damit du beim Übertragen der Antworten sofort die Stelle findest.

Tipp: Wer nicht gern tippt, kann diktieren – mit der Diktierfunktion des Handys (Mikrofon auf der Tastatur) oder unter Windows mit Win + H. Je nach Gerät wird die Sprache dabei vom Hersteller im Internet verarbeitet; Kennwörter und PINs deshalb lieber tippen.

Digitaler Nachlass bei den Diensten selbst

Viele große Dienste haben eigene Einstellungen für den Todesfall – bei Google der Kontoinaktivität-Manager, bei Apple und Facebook der Nachlasskontakt. Dort legst du fest, wer später an deine Daten kommt oder ob das Konto gelöscht wird. Das ersetzt Keyfiler nicht, ergänzt es aber: Im Vorsorgeordner hältst du in der Zeile Nachlasskontakt fest, ob du es beim jeweiligen Dienst eingerichtet hast. Wo genau die Einstellung steht, ändern die Anbieter gelegentlich – im Zweifel findest du sie in der Hilfe des Dienstes unter dem genannten Begriff.

Trifft nicht zu

Hast du zum Beispiel keine Berufsunfähigkeitsversicherung, wähle im Menü ⋯ des Dokuments Trifft nicht zu. Es bleibt erhalten, erscheint blass und zählt nicht mehr mit. Trifft zu nimmt das zurück.

Das geht auch für einen ganzen Ordner, zum Beispiel Haustiere oder Beruf und Geschäft: Wähle im Menü ⋯ des Ordners Trifft nicht zu. Dann gilt das für alles darin, und die Übersicht zeigt den Bereich blass. Nimmst du es zurück, gelten wieder die Markierungen der einzelnen Dokumente.

Bereiche löschen und wieder hinzufügen

Bereiche, die nicht zutreffen – etwa Haustiere oder Beruf und Geschäft –, löschst du wie jeden Ordner. Brauchst du sie später doch, findest du sie in der Übersicht unter Nicht in diesem Vorsorgeordner oder im Menü des Tresors unter Fehlende Bereiche hinzufügen …. Dort kannst du auch einzelne gelöschte Dokumente neu anlegen. Umbenennen und Verschieben ist jederzeit möglich; Keyfiler erkennt die vorbereiteten Teile trotzdem wieder.

Im Notfall lesbar machen

Damit deine Angehörigen im Ernstfall an den Vorsorgeordner kommen, richte einen Notfallzugang ein: Vertrauenspersonen fordern ihn bei Bedarf an und dürfen nach einer Wartezeit lesen.

Wichtig: Vollmachten, Verfügungen und Testamente wirken nur im unterschriebenen Original. Im Vorsorgeordner hältst du fest, wo sie liegen. Bei Fragen helfen zum Beispiel ein Notar oder die Betreuungsbehörde.

VORSORGE

Notfallzugang

Für einen Vorsorgeordner legst du Vertrauenspersonen fest, die ihn im Notfall lesen dürfen – zum Beispiel deinen Partner oder deine Kinder. Sie fordern den Zugang bei Bedarf an; du bekommst eine E-Mail und kannst während einer Wartezeit ablehnen. Danach dürfen sie lesen, ändern können sie nichts. Ein Notfallzugang lässt sich für jeden eigenen Vorsorgeordner einrichten.

Vertrauensperson einladen

1. Klick am Vorsorgeordner auf ⋯ (oder rechte Maustaste) und wähle Notfallzugang – oder unter Einstellungen › Vorsorge bei Notfallzugang auf Verwalten …
2. Wähle Vertrauensperson einladen …, gib an, für wen der Link ist (nur für dich sichtbar), und wähle die Wartezeit: Sofort, 1 bis 30 Tage oder mit Andere … bis zu 365 Tage.
3. Link erzeugen, dann Link kopieren, Von Keyfiler senden … oder Mit eigenem E-Mail-Programm …. Er gilt einmal und 7 Tage lang. Verschickt Keyfiler die Einladung, steht der Versand in deinem Protokoll (Einstellungen › Protokoll) – ohne den Code aus dem Link.

Ob die Person schon ein Keyfiler-Konto hat, musst du nicht wissen: Der Link funktioniert in beiden Fällen. Wer ihn öffnet, landet auf der Anmeldeseite und meldet sich mit seinem Konto an – oder wählt Noch kein Keyfiler-Konto? Konto anlegen und legt sich ein Konto nur für den Notfallzugang an.

Eine Vertrauensperson sieht immer den ganzen Vorsorgeordner. Soll jemand nur einen Teil sehen – etwa dein Geschäftspartner nur Beruf und Geschäft –, leg dafür einen zweiten Vorsorgeordner an, lösche dort die übrigen Bereiche und richte den Notfallzugang nur dort für diese Person ein.

Jede Vertrauensperson hat ihre eigene Wartezeit; bis zu 10 Personen je Vorsorgeordner sind möglich. Die Wartezeit änderst du später mit Wartezeit ändern …

> **„Sofort“ heißt: ohne Wartezeit.** Wer anfordert, kann gleich lesen – du hast keine Gelegenheit abzulehnen. Wähle das nur für Menschen, denen du voll vertraust.

Bestätigen – erst dann gilt der Zugang

Hat die Person angenommen, bekommst du eine E-Mail, und oben in der App erscheint ein Hinweis. Mit `Bestätigen …` siehst du den Fingerabdruck ihres Schlüssels. Vergleiche ihn mit der Person – am Telefon oder persönlich; sie findet ihn unter `Einstellungen` › `Konto`. Stimmt er, bestätige. Dein Browser verschlüsselt dabei den Schlüssel des Vorsorgeordners so, dass nur diese Person ihn öffnen kann. Der Server bewahrt ihn auf, gibt ihn aber erst nach Anforderung und Wartezeit heraus. Der Link selbst enthält keinen Schlüssel.

Danach bietet Keyfiler an, ein **Blatt für die Vertrauensperson** zu drucken (später auch über `Blatt drucken …`): Es erklärt, wo Keyfiler zu finden ist und wie der Zugang im Notfall angefordert wird. Zugangsdaten stehen nicht darauf.

Weitere Tresore freigeben

Manches steht nicht im Vorsorgeordner – etwa ein Tresor mit hunderten Zugangsdaten, die du nicht alle hineinkopieren möchtest. Mit `Weitere Tresore …` bei einer bestätigten Vertrauensperson wählst du eigene Tresore aus, die zusammen mit dem Vorsorgeordner freigegeben werden – ein Klick links schiebt einen Tresor nach rechts zu den freigegebenen, ein Klick rechts nimmt ihn wieder heraus. Wird der Vorsorgeordner freigegeben, erscheinen auch diese Tresore bei der Person – nur zum Lesen. Lehnst du ab oder beendest du den Zugriff, gilt das für alle zusammen.

Das legst du für jede Vertrauensperson einzeln fest – dein Partner bekommt vielleicht auch die Zugangsdaten, deine Kinder nur den Vorsorgeordner. Neue Personen musst du dafür nicht einladen: Dein Browser verschlüsselt den Schlüssel des Tresors direkt für die bestätigte Person. Bis zur Freigabe erfährt sie nichts davon.

> **Wähle die Wartezeit mit Bedacht.** Nach der Freigabe kann die Person alles darin lesen. Bei `Sofort` geht das ohne Vorwarnung. Löst du einen Tresor wieder, kann sie ihn nicht mehr öffnen; was schon angesehen wurde, lässt sich nicht zurückholen – im Zweifel den Tresor neu verschlüsseln.

Vorschau: Was sieht meine Vertrauensperson?

Mit `Vorschau …` bei einer bestätigten Vertrauensperson siehst du zuerst, welche Tresore sie im Notfall bekäme und welche nicht. `Vorschau starten` zeigt dir die App dann so, wie sie sich ihr zeigen würde: nur der Vorsorgeordner und die weiteren freigegebenen Tresore, alles nur zum Lesen, und deine Nachricht an die Vertrauenspersonen erscheint zuerst. So prüfst du, ob für den Ernstfall wirklich alles da ist. Es wird dabei nichts freigegeben. Damit du die Vorschau nicht mit deiner eigenen Arbeitsumgebung verwechselst, hat sie einen Rahmen in Bernstein und quer über den Bildschirm den Schriftzug „Notfallzugang“; oben steht eine Leiste mit `Beenden`, die dich zurückbringt.

Im Notfall: Zugang anfordern

1. Die Vertrauensperson meldet sich mit ihrem eigenen Konto an und klickt in der Seitenleiste unten auf `Notfallzugänge`.
2. Beim Vorsorgeordner wählt sie `Zugang anfordern …` und schreibt auf Wunsch kurz, was passiert ist.
3. Du bekommst sofort eine E-Mail mit dem Tag, ab dem sie lesen kann. In der App öffnest du mit `Ansehen` den Notfallzugang und wählst `Ablehnen` oder – wenn alles in Ordnung ist – `Freigeben`, damit sie nicht warten muss.
4. Lehnst du nicht ab, darf sie nach Ablauf der Wartezeit lesen. Der Vorsorgeordner erscheint dann in ihrer Seitenleiste mit dem Notfall-Symbol am rechten Rand – nur zum Lesen, Drucken und Kopieren. Hast du eine Nachricht an deine Vertrauensperson(en) geschrieben, weist Keyfiler sie beim Öffnen zuerst darauf hin.

Eine Anforderung kann die Vertrauensperson jederzeit zurückziehen. Mit `Zugriff beenden` nimmst du einen freigegebenen Zugang wieder zurück; die Person bleibt Vertrauensperson und kann erneut anfordern. Ein automatisches Freigeben nach längerer Inaktivität gibt es nicht.

Entfernen und zurücktreten

- Mit dem × entfernst du eine Vertrauensperson oder ziehst eine offene Einladung zurück. Hatte sie schon Lesezugriff, ist Tresor neu verschlüsseln vorausgewählt – wie beim Entziehen eines gemeinsamen Tresors. Die übrigen Vertrauenspersonen behalten ihren Zugang.
- Eine Vertrauensperson kann unter Notfallzugänge mit dem × zurücktreten; du bekommst dann eine E-Mail. Ebenso, wenn sie ihr Konto löscht.

Konten von Vertrauenspersonen

Wer über einen Notfall-Link ein neues Konto anlegt, kann damit keine eigenen Tresore anlegen – die Begrüßung führt direkt zu den Notfallzugängen. Ist der Wiederherstellungsschlüssel aufbewahrt, zeigt die Startseite statt der Begrüßung Deine Notfallzugänge: für wen man Vertrauensperson ist und wie der Stand ist. Ein Admin kann das unter Administration › Benutzer mit Eigene Tresore erlauben ändern; solche Konten tragen dort das Kennzeichen Vertrauensperson.

> **Kein Ersatz für eine Vollmacht.** Der Notfallzugang gibt Einblick in deine Unterlagen. Rechtlich handeln darf die Person damit noch nicht – dafür brauchst du eine Vorsorgevollmacht.

4 Dokumente

DOKUMENTE

Aufbau eines Dokuments

Ein Dokument besteht aus beliebig vielen Zeilen. Du entscheidest selbst, welche Angaben es enthält – ein Login braucht andere Zeilen als ein Vertrag oder ein Router.

Kopf anheften

Am Computer und Tablet bleibt der Kopf eines Dokuments – Titel, Knöpfe, Pfad und Datum – beim Scrollen oben stehen. Mit der Stecknadel unten rechts im Kopf (oder ⋯ › Kopf lösen) scrollt er mit und lässt mehr Platz für den Inhalt; erneut klicken heftet ihn wieder an. Am Handy scrollt er anfangs mit. Die Wahl gilt für dieses Gerät.

Die Zeilenarten

- **Zeile:** Bezeichnung und Inhalt, zum Beispiel „Benutzer“ und „max.mustermann“. Inhalte lassen sich verdecken – für Kennwörter, PINs und Ähnliches. Webadressen und E-Mail-Adressen kannst du direkt öffnen.
- **Überschrift:** gliedert ein längeres Dokument, etwa in „Online-Banking“ und „Konto“.
- **Zwischenraum:** ein Abstand zwischen Gruppen von Zeilen.
- **Notiz:** ein längerer, mehrzeiliger Text.
- **Datum** und **Uhrzeit:** mit Kalender bzw. Uhrzeitauswahl, angezeigt als „05.03.2024“ bzw. „14:30 Uhr“ – etwa für „Gültig bis“ oder einen Termin.
- **Ja/Nein:** zwei Knöpfe zur Auswahl, auch direkt in der Ansicht; ein zweiter Klick auf die gewählte Antwort lässt die Frage wieder offen.
- **Ankreuzen:** ein Kästchen, das du auch in der Ansicht direkt an- und abhakst – praktisch für Erledigtes.
- **2FA-Code:** erzeugt Zwei-Faktor-Codes – siehe 2FA-Codes in Dokumenten.
- **Betrag:** tippe, wie du es gewohnt bist – „1234,5“, „1.234,50“ oder „1234.50“. Keyfiler zeigt daraus „1.234,50 EUR“. Zum Ändern der Währung klickst du beim Bearbeiten auf das Kürzel im Feld (oder Zeilenmenü ⋯ › Währung). Fehlt eine in der Liste, findest du unter Andere Währung … alle Währungen der Welt – tippe den Namen oder das Kürzel, etwa „Austral“ oder „AUD“. Schon benutzte Währungen stehen danach mit in der Liste.
- **IBAN** und **BIC:** Groß- und Kleinschreibung und Leerzeichen sind egal; die IBAN erscheint in Vierergruppen. Ein Haken zeigt, dass die Prüfziffer stimmt; bei einem Zahlendreher wird das Feld rot und ein Hinweis erscheint. Gespeichert wird trotzdem.
- **Kartennummer:** in Gruppen, mit Prüfung der Prüfziffer; neu angelegt wie ein Kennwort verdeckt.

Kopierst du eine IBAN oder Kartennummer, kommt sie ohne Leerzeichen in die Zwischenablage – so, wie Banking-Seiten sie erwarten. Alle Prüfungen laufen in deinem Browser; nichts verlässt dein Gerät.

Art einer Zeile ändern

Im Zeilenmenü ⋯ am Ende jeder Zeile (oder Umschalt + F10) wählst du unter Art, welche Art eine Zeile hat: Text, Notiz (mehrzeilig), Termin, Datum, Uhrzeit, Betrag, IBAN, BIC, Kartennummer oder 2FA-Code – etwa für importierte Daten. Aus „31.12.2026“ wird so eine Datumszeile mit Kalender (bei „12/27“ der Monatsletzte), aus „14.30 Uhr“ eine Uhrzeit, aus einem geheimen Schlüssel ein 2FA-Code. Eine Notiz mit mehreren Zeilen bleibt Notiz. Steht in einer Zeile wie „Datum“ ein Datum als Text, schlägt Keyfiler In Datum umwandeln vor, bei „Gültig bis“ & Co. In Termin umwandeln (siehe Termine). Lässt sich ein Inhalt nicht umwandeln, zum Beispiel „ca. 500 Euro“ als Betrag, bleibt die Zeile Text. Steht in einer normalen Zeile eine gültige IBAN – egal, wie die Zeile heißt –, schlägt Keyfiler direkt unter dieser Zeile vor, sie als IBAN zu formatieren. Bei BIC, Kartennummer und Beträgen geschieht das, wenn auch die Bezeichnung passt (z.B. „BIC“, „Kartennummer“, „Betrag“). Nein danke blendet den Vorschlag für diese Zeile aus.

Darunter stehen die **Bemerkungen** für alles Weitere und die Anhänge.

Bearbeiten

1. Klicke auf Bearbeiten oder drücke F2.
2. Füge Zeilen über die Knöpfe Zeile, Überschrift, Notiz, Datum, Betrag und IBAN hinzu; unter Weitere … stehen Zwischenraum, Uhrzeit, Ja/Nein, Ankreuzen, BIC, Kartennummer und 2FA-Code. Ein Klick fügt die neue Zeile unter der Zeile ein, in der gerade der Cursor steht, sonst am Ende. Du kannst die Knöpfe – auch die Einträge unter Weitere … – aber auch direkt an die gewünschte Stelle ziehen; eine rote Linie mit Pfeilen an beiden Enden zeigt, wo die Zeile entsteht. Strg + Enter fügt eine neue Zeile direkt darunter ein.
3. Schreibe den Inhalt in die Felder rechts. Ein Klick auf die Bezeichnung links setzt den Cursor ebenfalls dorthin. Mit Tab oder Enter springst du von Inhalt zu Inhalt (in Notizen macht Enter eine neue Zeile). In der letzten Zeile hängt Enter eine neue Zeile an, sobald die letzte etwas enthält – so tippst du ein Dokument in einem Zug herunter. Die Symbole rechts (Verdecken, Überschrift, Löschen …) und Inhalt leeren erreichst du per Tastatur mit Umschalt + F10.
4. **Bezeichnung ändern:** Vorhandene Bezeichnungen sind geschützt, damit du nicht aus Versehen hineinschreibst. Zum Umbenennen klickst du auf das Umbenennen-Symbol, das beim Überfahren der Zeile erscheint (auf Handy und Tablet immer sichtbar), doppelklickst auf die Bezeichnung oder drückst F2 in der Zeile. Enter übernimmt, Esc stellt die alte Bezeichnung wieder her – ebenso, wenn du das Feld leer verlässt. Neue Zeilen kannst du sofort beschriften.
5. Das × rechts im Feld leert den Inhalt – bei normalen und verdeckten Zeilen, 2FA-Schlüsseln, Datum und Uhrzeit. Vertan? Rückgängig in der Meldung oder Strg + Z holt ihn zurück.
6. Eine Zeile löschst du mit dem Papierkorb rechts oder im Menü ⋯. Keyfiler fragt nicht nach, sondern zeigt unten Rückgängig an (auch Strg + Z). Mit ⋯ › Duplizieren entsteht eine Kopie der Zeile direkt darunter – praktisch für wiederkehrende Angaben wie mehrere Kontakte oder Geräte.
7. Leere Zeilen ohne Bezeichnung und Inhalt räumt Keyfiler bei Fertig von selbst weg. Zwischenräume und vorbereitete Zeilen mit Hinweis (z.B. im Vorsorgeordner) bleiben stehen.
8. Die Symbole rechts in den Zeilen klappst du mit Symbole am Ende der Linie „Angaben“ ein und aus. Eingeklappt bleibt nur ⋯ – darin stehen alle Aktionen der Zeile, auch Kopieren –, und die Felder für den Inhalt werden breiter. Keyfiler merkt sich die Wahl auf diesem Gerät.
9. Ziehe Zeilen am Griff an eine andere Stelle oder verschiebe sie mit Alt + ↑ / ↓. Lässt du in der oberen Hälfte einer Zeile los, landet sie davor, in der unteren Hälfte dahinter – so geht es auch ganz ans Ende.
10. Klicke auf Fertig oder drücke Esc.

Mehrere Zeilen auf einmal

Beim Bearbeiten wählst du Zeilen mit einem Klick auf den **Griff** links aus; ein zweiter Klick nimmt sie wieder heraus. Mit Umschalt + Klick wählst du alle Zeilen bis zur zuletzt angeklickten. Auf dem Handy geht es über das Zeilenmenü ⋯ › Auswählen. Ausgewählte Zeilen sind grün hinterlegt, und über den Zeilen erscheint eine Leiste:

- Kopieren (Strg + C): Danach klickst du auf die Zeile, unter der die Kopien stehen sollen – eine rote Linie mit kleinen Pfeilen an beiden Enden zeigt die Stelle, über der ersten Zeile steht Hier ganz oben einfügen. Esc oder Abbrechen beendet das Zeigen.
- Ausschneiden (Strg + X) funktioniert genauso, nur werden die Zeilen **verschoben**: Bis zum Einfügen bleiben sie blass an ihrem Platz; brichst du ab, bleibt alles, wie es war.
- **In ein anderes Dokument:** Öffne es zum Bearbeiten – oben steht dann … Zeilen in der Zwischenablage. Mit Einfügen … zeigst du auf die Stelle. Das geht auch in einem anderen Tresor; ausgeschnittene Zeilen aus einem anderen Tresor werden dabei kopiert und bleiben im Ursprung stehen.
- Strg + V fügt ohne Zeigen direkt unter der Zeile mit dem Cursor ein.

- Die Keyfiler-Zwischenablage liegt nur im Arbeitsspeicher deines Browsers, nicht in der Zwischenablage deines Geräts – verdeckte Inhalte gelangen so nicht in andere Programme. Sie leert sich nach 5 Minuten, beim Sperren und beim Abmelden; das ✕ in der Leiste leert sie sofort.
- Als Text kopiert die Zeilen als „Bezeichnung: Inhalt“ in die Zwischenablage deines Geräts, etwa für eine E-Mail. Sind verdeckte Inhalte dabei, fragt Keyfiler, ob sie mitsollen. Nach 30 Sekunden wird die Zwischenablage geleert.
- Löschen (Entf) entfernt die Zeilen; Rückgängig holt sie an ihre alten Stellen zurück. Ab 5 Zeilen fragt Keyfiler vorher nach.
- Nach oben und Nach unten verschieben den Block um eine Zeile, ✕ hebt die Auswahl auf (Esc). Ziehst du eine ausgewählte Zeile am Griff, wandern alle ausgewählten mit. Eine einzelne Zeile kopierst du direkt darunter mit ⋯ › Duplizieren.
- Kopierst du eine 2FA-Zeile, kommt ihr Schlüssel mit – der Code gilt dann auch im neuen Dokument.

Vorschläge für Bezeichnungen und Inhalte erscheinen erst, wenn du tippst (oder mit ↓) – ein Klick ins Feld allein öffnet keine Liste.

Inhalte kopieren

Ein Klick auf eine Zeile kopiert ihren Inhalt, auch verdeckte. Per Tastatur wählst du die Zeile mit ↑ / ↓ und kopierst mit Enter. Leere Zeilen zeigen blass (leer) – dort wird nichts kopiert.

DOKUMENTE

Dokumentvorlagen

Dokumentvorlagen geben neuen Dokumenten ihre Zeilen vor. Legst du zum Beispiel regelmäßig Webhosting-Zugänge an, brauchst du die Zeilen „Anbieter“, „Benutzer“, „Kennwort“ und „Kundennummer“ nur einmal zu definieren.

Vorlage erstellen

1. Lege ein Dokument mit den gewünschten Zeilen an – oder nimm ein vorhandenes.
2. Öffne sein Menü ⋯ und wähle Als Vorlage speichern.

Legst du ein neues Dokument an, wählst du im Feld Vorlage die passende aus – eine Vorschau zeigt ihre Zeilen. Gespeichert werden nur die Zeilen, keine Inhalte. Keyfiler bringt außerdem einige Standardvorlagen mit, dazu die Gruppe Vorsorge für den Vorsorgeordner. Die Vorsorge-Vorlagen lassen sich nicht ändern; speichere ein damit angelegtes Dokument als eigene Vorlage, wenn du sie anpassen möchtest.

Vorlagen verwalten

Unter Einstellungen › Dokumentvorlagen › Vorlagen verwalten … benennst du Vorlagen um oder löschst sie. Vorlagen gelten für alle deine Tresore und sind in jeder Sicherung enthalten.

DOKUMENTE

Anhänge

An jedes Dokument kannst du Dateien anhängen – etwa den Vertrag als PDF, einen Versicherungsschein oder den Scan eines Ausweises. Anhänge werden genauso verschlüsselt wie alles andere, bevor sie dein Gerät verlassen.

Anhang hinzufügen und öffnen

- **Hinzufügen:** Unter dem Dokument Dateien in das Feld Dateien hierher ziehen oder auswählen ziehen oder darauf klicken. Während Keyfiler die Dateien verschlüsselt und hochlädt, steht an dieser Stelle ein Fortschrittsbalken mit Prozent und Größe; mit Abbrechen hältst du an – was noch nicht vollständig angekommen ist, wird nicht gespeichert. Schließt du den Tab, solange noch hochgeladen wird, fragt der Browser vorher nach.
- **Vorschau:** Bilder (JPG, PNG, GIF, WebP), PDFs, Textdateien, Tabellen (Excel .xlsx, LibreOffice .ods, CSV) und Word-Dokumente (.docx) zeigt Keyfiler direkt in der App – Klick auf den Namen oder das Auge. Bei mehreren Anhängen blätterst du mit ← / → oder den Pfeilen

links und rechts. Die Pfeile blenden sich nach kurzer Zeit aus, damit sie nichts verdecken; sie erscheinen wieder, wenn du mit der Maus an den linken oder rechten Rand gehst oder auf den Bildschirm tippst. Entschlüsselt wird nur in deinem Browser, gespeichert wird dabei nichts.

- **Bilder vergrößern:** Mit der Lupe oben (− / +), dem Mausrad oder + / −; das Mausrad zoomt an die Stelle unter dem Mauszeiger. Ein Doppelklick wechselt zwischen eingepasst und Originalgröße, ein Klick auf die Prozentzahl oder 0 passt das Bild wieder ein. Ist das Bild größer als das Fenster, verschiebst du es mit gedrückter Maustaste. Auf dem Handy zoomst du mit zwei Fingern oder doppeltem Tippen.
- **Bilder drehen:** Liegt ein Foto oder Scan quer, dreht das Symbol mit dem Pfeil oben in der Vorschau (oder R) es um 90° im Uhrzeigersinn. Mit Gedreht speichern wird das gedrehte Bild zur neuen Fassung des Anhangs – danach liegt es überall richtig, auch beim Herunterladen und Drucken. PNG bleibt dabei verlustfrei, JPG und WebP werden in hoher Qualität neu gespeichert; Angaben der Kamera (z.B. ein gespeicherter Aufnahmeort) fallen dabei weg. GIF-Bilder kannst du nur in der Vorschau drehen. Wer einen gemeinsamen Tresor nur lesen darf, kann drehen, aber nicht speichern.
- **Tabellen:** Mehrere Blätter erscheinen als Reiter. Spaltenbuchstaben und Zeilennummern bleiben beim Scrollen stehen; Datum, Euro- und Prozentwerte sind deutsch dargestellt; fett, verbundene Zellen, Ausrichtung und Zeilenumbruch übernimmt die Vorschau aus der Datei. Bei Formeln zeigt Keyfiler das Ergebnis, das Excel oder LibreOffice beim Speichern mit abgelegt hat – nachgerechnet wird nicht. Diagramme und Bilder in Tabellen sowie die alten Formate .xls und .doc zeigt die Vorschau nicht. Sehr große Blätter erscheinen in Schritten, höchstens 5.000 Zeilen und 200 Spalten.
- **Word-Dokumente:** Keyfiler zeigt Text, Überschriften, fett und kursiv, Aufzählungen, Tabellen und Bilder auf einem weißen Blatt – als Lesefassung, nicht seitengenau wie in Word. Kopf- und Fußzeilen, Kommentare, Textfelder und Diagramme fehlen; bei Änderungsverfolgung siehst du den Text mit allen Änderungen. Links zeigt Keyfiler nur an (Adresse beim Darüberfahren), geöffnet wird nichts. Mit Kennwort geschützte Dokumente öffnest du in Word.
- **Neue Fassung hochladen:** Das Symbol mit den Pfeilen oben in der Vorschau ersetzt den Anhang durch eine neue Datei, etwa nachdem du die Tabelle in Excel bearbeitet hast. Bearbeiten selbst geht weiter in Excel, LibreOffice oder Word.
- **Umbenennen, neue Fassung, löschen:** Über ⋯ am Anhang. Umbenennen … gibt ihm einen neuen Namen; die Endung (z.B. .pdf) bleibt, wenn du sie weglässt. Fotos, die du am Handy direkt mit der Kamera aufnimmst, heißen zunächst Foto mit Datum und Uhrzeit, etwa Foto 21.11.2026 22-09.jpg .
- **Am Handy:** Auch Vorschau und Herunterladen findest du hinter ⋯ am Anhang – so bleibt der Name lesbar.
- **Herunterladen oder in neuem Tab:** Über die Symbole oben in der Vorschau oder neben dem Anhang. Tabellen und Word-Dokumente kann der Browser nicht selbst öffnen, sie lädst du herunter. Andere Dateitypen lädst du direkt herunter.
- **Fenster anpassen:** Am Computer verschiebst du die Vorschau an der Kopfzeile, ziehst sie am Winkel unten rechts größer und vergrößerst sie mit dem Pfeil-Symbol (oder Doppelklick auf die Kopfzeile) auf die ganze Seite. Die Größe merkt sich der Browser.
- **PDF auf dem Handy:** Manche Handy-Browser (z.B. Chrome auf Android) zeigen PDFs nicht in der App an. Die Vorschau bietet dann Öffnen und Herunterladen an. Auf dem Handy öffnest du die Vorschau mit einem Tipp auf den Namen.

Reihenfolge ändern

Hat ein Dokument mehrere Anhänge, steht links an jedem ein Griff ⋮⋮. Fass ihn an und zieh den Anhang an eine andere Stelle – mit der Maus oder mit dem Finger. Eine rote Linie zeigt, wo er landet; stehen die Anhänge nebeneinander, steht sie senkrecht zwischen zwei Anhängen. Mit der Tastatur steuerst du den Griff mit Tab an und verschiebst mit ↑ und ↓. Die Reihenfolge wird sofort gespeichert und gilt für alle, die das Dokument sehen. Wer einen gemeinsamen Tresor nur lesen darf, sieht keinen Griff.

Neue Fassung hochladen

Pflegst du eine Datei weiter – etwa eine Kostenübersicht in Excel –, musst du den alten Anhang nicht löschen. Der Anhang behält seinen Platz, nur der Inhalt wird ersetzt:

- **Gleicher Name:** Zieh die geänderte Datei wie gewohnt auf Dateien hierher ziehen oder auswählen . Gibt es schon einen Anhang mit diesem Namen, fragt Keyfiler: Ersetzen oder Zusätzlich anhängen .
- **Auf den Anhang ziehen:** Zieh die Datei direkt auf den Anhang, der ersetzt werden soll – er wird grün umrandet.

- **Mit dem Knopf:** Die kreisenden Pfeile neben dem Anhang öffnen die Dateiauswahl. Hat die neue Datei einen anderen Namen, bleibt der bisherige, außer du setzt das Häkchen Neuen Dateinamen übernehmen.

Unter dem Namen steht danach neue Fassung vom …, in einem gemeinsamen Tresor auch, wer sie hochgeladen hat. Die bisherige Fassung wird überschrieben und lässt sich nicht zurückholen – Keyfiler ersetzt sie aber erst, wenn die neue vollständig angekommen ist. Hat inzwischen jemand anderes eine neuere Fassung hochgeladen, lehnt Keyfiler deine ab und lädt das Dokument neu, damit nichts unbemerkt verloren geht. Wer einen gemeinsamen Tresor nur lesen darf, kann keine neue Fassung hochladen.

Wie viel Platz habe ich?

Unter Einstellungen › Konto siehst du bei Speicher für Anhänge, wie viel du schon belegst und wie viel dir zur Verfügung steht.

Achtung bei gespeicherten Dateien: Ein heruntergeladener oder in einem neuen Tab geöffneter Anhang liegt unverschlüsselt auf deinem Gerät. Lösche ihn dort wieder, wenn du ihn nicht mehr brauchst – besonders auf fremden Rechnern.

DOKUMENTE

2FA-Codes in Dokumenten

Viele Dienste bieten eine Zwei-Faktor-Anmeldung mit einer Authenticator-App an. Keyfiler kann diese Codes selbst erzeugen: Du siehst den aktuellen Code direkt im Dokument neben Benutzername und Kennwort.

So richtest du es ein

1. Schalte beim jeweiligen Dienst die Zwei-Faktor-Anmeldung ein. Er zeigt dir einen QR-Code und meist auch einen Schlüssel zum Abtippen (oft unter „Code kann nicht gescannt werden?“).
2. Öffne in Keyfiler das passende Dokument, klicke auf Bearbeiten und füge eine Zeile 2FA-Code hinzu.
3. Trage den Schlüssel des Dienstes ein und klicke auf Fertig.
4. Keyfiler zeigt jetzt den aktuellen sechsstelligen Code. Gib ihn beim Dienst zur Bestätigung ein.

Ein Klick auf die Zeile kopiert den aktuellen Code, per Tastatur geht es mit Strg + Umschalt + C.

Bequem, aber bewusst entscheiden: Liegen Kennwort und zweiter Faktor im selben Tresor, schützt die Zwei-Faktor-Anmeldung eines Dienstes nicht mehr vor jemandem, der deinen Keyfiler öffnen kann. Für besonders wichtige Konten, etwa E-Mail oder Bank, kann eine separate Authenticator-App auf dem Handy sinnvoller sein.

Die Zwei-Faktor-Anmeldung für Keyfiler selbst richtest du nicht hier ein, sondern in den Einstellungen – siehe Zwei-Faktor-Anmeldung einrichten.

DOKUMENTE

Passwort-Generator

Der Generator erzeugt zufällige, starke Kennwörter. Du öffnest ihn beim Bearbeiten eines Dokuments an einer Kennwort-Zeile oder mit Strg + Umschalt + G – dann trägt Übernehmen das Kennwort in die Zeile ein. Brauchst du nur schnell ein Kennwort, etwa für ein neues Konto bei einem Dienst, öffnest du ihn über das Kontomenü unten links: Passwort-Generator. Dort legt Kopieren und schließen das Kennwort in die Zwischenablage; nach 30 Sekunden wird sie wieder geleert.

Einstellungen

- **Länge:** 4 bis 128 Zeichen, voreingestellt sind 20.

- **Zeichenarten:** A–Z, a–z, 0–9 und Sonderzeichen. Welche Sonderzeichen erlaubt sind, legst du im Feld daneben fest – praktisch, wenn ein Dienst bestimmte Zeichen nicht akzeptiert.
- **Stärke:** Unter dem Kennwort zeigt ein Balken in fünf Stufen, wie stark es ist – von Sehr schwach (rot) über Mittel (gelb) bis Sehr stark (grün). Daneben steht die Zufälligkeit in Bit: Je mehr, desto länger bräuchte ein Angreifer zum Erraten. Ab etwa 75 Bit gilt ein Kennwort als stark.

Eigenes Muster

Mit Vorlage verwenden gibst du den Aufbau selbst vor, zum Beispiel Cvccvc-99-Cvccvc. So entstehen Kennwörter, die sich leichter abtippen oder vorlesen lassen.

- **A / a** – Buchstabe (groß / klein)
- **C / c** – Konsonant, **V / v** – Vokal
- **9** – Ziffer, **$** – Sonderzeichen
- alle anderen Zeichen bleiben so stehen

DOKUMENTE

Termine

Keyfiler erinnert dich an Termine in deinen Dokumenten – etwa wann der Personalausweis abläuft, bis wann ein Vertrag gekündigt werden muss oder wann die nächste Rate fällig ist.

Termin eintragen

- **Neue Zeile:** Beim Bearbeiten unten auf Termin klicken. Eintragen kannst du ein Datum (31.12.2026), ein Datum mit Uhrzeit (31.12.2026 14:30) oder nur Monat und Jahr (12/2026, gilt bis Monatsende – wie auf Kreditkarten). Rechts im Feld öffnet der Kalender die Datumsauswahl, die Glocke Status und Vorlauf.
- **Vorhandene Zeile umwandeln:** Im Zeilenmenü ⋯ › Art › Termin. Steht in einer Zeile wie „Gültig bis“, „Kündigen bis“ oder „TÜV“ schon ein Datum, schlägt Keyfiler darunter In Termin umwandeln vor – und die Übersicht bietet an, alle solchen Zeilen auf einmal umzuwandeln.
- **Vorlauf:** Wie früh Keyfiler erinnert, stellst du je Termin ein: am Tag selbst, 1 oder 2 Wochen, 30 (Standard), 60, 90 oder 180 Tage vorher. Beim Reisepass sind 90 Tage sinnvoll, damit ein neuer rechtzeitig da ist.
- Eine normale Zeile der Art Datum – etwa das Geburtsdatum – erinnert nie.

Offen, erledigt, ignorieren

Im Dokument steht neben dem Termin, wie lange es noch dauert (in 12 Tagen, abgelaufen). Ein Klick darauf öffnet ein Menü: Offen, Erledigt oder Ignoriert – und den Vorlauf. Beim Bearbeiten findest du dasselbe hinter der Glocke im Feld und im Zeilenmenü ⋯ unter Termin.

- **Erledigt** heißt: Darum hast du dich gekümmert. Keyfiler erinnert nicht mehr.
- **Ignoriert** heißt: Dieser Termin interessiert dich nicht – er erscheint nirgends mehr.
- Beides gilt nur für das eingetragene Datum. Trägst du ein neues ein, etwa nach dem Verlängern, ist der Termin wieder offen. Es gilt für alle, die den Tresor sehen.

Übersicht „Termine“

- **Öffnen:** im Kontomenü ⋯ unten in der Seitenleiste unter Termine oder im Schnellzugriff.
- **Inhalt:** Abgelaufen, Steht an (der Vorlauf ist erreicht) und Demnächst (bis 90 Tage). Ein Klick auf die Markierung eines Eintrags (z.B. abgelaufen) setzt ihn auf erledigt oder ignoriert und ändert den Vorlauf. Erledigt ist zugeklappt und zeigt die letzten 30 Tage. Ein Klick

auf einen Eintrag öffnet das Dokument.

- **Hinweis oben:** Ist ein Termin abgelaufen oder steht er an, erscheint nach der Anmeldung ein Hinweis. Später blendet ihn für eine Woche aus. Abschalten: Einstellungen › Darstellung › An Termine erinnern.
- Berücksichtigt werden alle Tresore, aber nicht der Papierkorb. In Tresoren, die du nur lesen darfst, kannst du den Status nicht ändern.

5 Schneller arbeiten

SCHNELLER ARBEITEN

Schnellzugriff und Favoriten

Der Schnellzugriff ist der schnellste Weg zu jedem Dokument – egal, in welchem Tresor es liegt.

1. Drücke Strg + K.
2. Tippe ein paar Buchstaben. Keyfiler sucht in allen Tresoren nach Dokumenten, Tresoren und Befehlen.
3. Wähle mit ↑ / ↓ und öffne mit Enter.

Noch schneller: Strg + Enter kopiert direkt das Kennwort des gewählten Dokuments, Umschalt + Enter den Benutzernamen – ohne das Dokument zu öffnen.

Favoriten und zuletzt geöffnet

- **Favorit setzen:** Klicke im Dokument auf den Stern oder drücke Strg + D.
- Favoriten und zuletzt geöffnete Dokumente erscheinen oben in der Seitenleiste und im Schnellzugriff, solange das Suchfeld leer ist.
- Anfangs zeigt die Seitenleiste nur die Favoriten. „Zuletzt geöffnet“ schaltest du unter Einstellungen › Darstellung ein – erst dann merkt sich Keyfiler die geöffneten Dokumente. Beim Ausschalten wird die Liste gelöscht; die Favoriten lassen sich dort ebenfalls ausblenden.

SCHNELLER ARBEITEN

Switchboard

Das Switchboard zeigt eine Zeile des Dokuments groß an – praktisch, wenn du ein Kennwort abtippen musst, etwa am Fernseher, am Drucker oder an einem anderen Rechner, oder wenn du Anmeldename und Kennwort nacheinander in eine Anmeldeseite überträgst.

1. Ab einer bestimmten Zeile: Fahre mit der Maus über die Zeile und klicke auf das Symbol Switchboard rechts darin – oder drücke S, wenn die Zeile mit der Tastatur gewählt ist.
2. Ab der zuletzt angeklickten Zeile (sonst der ersten): ⋯ › Switchboard oben im Dokument oder im Schnellzugriff Switchboard.
3. Mit ↑ / ↓ gehst du durch die Zeilen; Überschriften und leere Zeilen werden übersprungen.
4. Übertragen: Strg + C oder das Kopier-Symbol kopiert den Inhalt (nach 30 Sekunden wird die Zwischenablage wieder geleert). Oder du ziehst den Inhalt am gestrichelten Griff rechts direkt in ein Eingabefeld – auch in ein anderes Fenster. Markieren mit der Maus geht ebenfalls.

- **Gut lesbar:** Ziffern sind grün, Sonderzeichen rot, Leerzeichen erscheinen als heller Punkt. Unter jedem Zeichen steht klein seine Stelle – so verzählt man sich bei langen Inhalten nicht. Beim Kopieren und Ziehen kommen nur die Zeichen mit.
- **Verdeckte Inhalte** wie Kennwort oder PIN bleiben verdeckt, bis du auf das Auge klickst. Dann sind alle verdeckten Zeilen des Dokuments sichtbar, bis du das Auge wieder schließt – bei einem anderen Dokument sind sie wieder zu. Kopieren und Ziehen geht auch verdeckt.
- **Nur Buchstaben und Ziffern:** Mit dem Häkchen fallen Leer- und Sonderzeichen weg – für Formulare, die etwa eine Lizenznummer oder IBAN nur ohne Bindestriche und Leerzeichen annehmen.
- **2FA-Codes** zeigt das Switchboard als aktuellen Code mit den verbleibenden Sekunden.

Schwebendes Fenster

In Chrome und Edge sowie in Firefox ab Version 151 öffnet sich das Switchboard am Computer als kleines eigenes Fenster, das über allen anderen Fenstern bleibt – auch wenn du Keyfiler minimierst oder ein anderes Programm davorholst. Die Größe änderst du an der Fensterecke; ein größeres Fenster zeigt größere Zeichen. Wo es das nicht gibt (Safari, Handy), erscheint das Switchboard als Fenster in der App. Esc schließt es; wechselst du zu einem anderen Dokument oder verlässt das Dokument, schließt es sich von selbst.

Beim Sperren und Abmelden schließt sich das Switchboard sofort. Bedenke beim Teilen deines Bildschirms, dass ein aufgedeckter Inhalt für alle sichtbar ist.

SCHNELLER ARBEITEN

Suchen

Keyfiler kennt zwei Arten zu suchen:

- **In allen Tresoren:** der Schnellzugriff mit Strg + K findet Dokumente, Tresore und Befehle überall.
- **Im geöffneten Tresor:** das Suchfeld über der Liste oder Strg + F.

Auch die Hilfe selbst lässt sich durchsuchen: Das Feld Hilfe durchsuchen steht oben über den Themen, im Hilfefenster springt Strg + F hinein. Groß- und Kleinschreibung spielt keine Rolle, „ue“ findet auch „ü“; bei mehreren Wörtern müssen alle vorkommen.

Auf dem Handy tippst du unten auf Suchen: Auf der Startseite mit den Tresoren öffnet das den Schnellzugriff für alle Tresore, in einem Tresor das Suchfeld über der Liste.

Gefundene Einträge sind immer im Baum sichtbar: Kategorie, Tresor und Ordner werden dafür automatisch aufgeklappt.

Gesucht wird ausschließlich in deinem Browser. Weil der Server deine Daten nicht lesen kann, erfährt er auch nicht, wonach du suchst.

SCHNELLER ARBEITEN

Tastenkürzel

Keyfiler lässt sich vollständig mit der Tastatur bedienen. ? zeigt die Übersicht der Tastenkürzel, F1 öffnet diese Hilfe – passend zu dem, was du gerade machst.

Handbuch: Alle Anleitungen gibt es auch als PDF zum Nachlesen oder Ausdrucken – im Hilfefenster oben über Handbuch herunterladen oder mit Strg + K → Handbuch herunterladen. Es gehört immer zur aktuellen Version der App.

Überall

F1	Hilfe öffnen (passend zum geöffneten Fenster)
?	Übersicht der Tastenkürzel
Strg + K	Schnellzugriff: Dokument, Tresor oder Befehl finden
Strg + F	Im geöffneten Tresor suchen (in der Hilfe: Hilfe durchsuchen)
F6 / Umschalt + F6	Zwischen Seitenleiste, Liste und Ansicht wechseln
Alt + ↑	Eine Ebene höher
Strg + P	Drucken
Strg + Umschalt + L	Sofort sperren (Mac: ⌘ + Umschalt + L)
Strg + Z	Verschieben, Kopieren oder Löschen rückgängig machen
Esc	Dialog, Menü oder Bearbeiten schließen

Alt + F8	Im Passwortfeld: Passwort anzeigen bzw. verbergen

Schnellzugriff

↑ / ↓	Treffer wählen
Enter	Öffnen bzw. ausführen
Strg + Enter	Kennwort des Dokuments kopieren
Umschalt + Enter	Benutzernamen kopieren

Seitenleiste und Liste

↑ / ↓	Eintrag wählen
Enter / →	Öffnen bzw. aufklappen
F2	Umbenennen bzw. Tresor bearbeiten
Einfg	Neues Dokument (in der Seitenleiste: neuer Tresor)
Strg + Einfg	Neuer Ordner
Entf	In den Papierkorb
Strg + Klick	Mehrere Einträge markieren
Strg + A	Alle Einträge markieren
Buchstaben	Zum Eintrag springen, der so anfängt

Dokument

↑ / ↓ und Enter	Zeile wählen und kopieren
F2	Bearbeiten; beim Bearbeiten: Bezeichnung der Zeile ändern
Strg + D	Favorit setzen oder entfernen
Strg + Umschalt + C	Inhalt der Zeile kopieren (bei 2FA: aktueller Code)
Strg + Enter	Beim Bearbeiten: neue Zeile darunter
Strg + Umschalt + G	Beim Bearbeiten: Passwort erzeugen (sonst über das Kontomenü › Passwort-Generator)
Alt + ↑ / ↓	Beim Bearbeiten: Zeile verschieben
Strg + C / X / V	Beim Bearbeiten: ausgewählte Zeilen kopieren, ausschneiden, Zeilen einfügen
Entf	Beim Bearbeiten: ausgewählte Zeilen löschen
Tab / Enter	Beim Bearbeiten: zum nächsten Inhalt (Umschalt dazu: zurück)
Umschalt + F10 / Kontextmenü-Taste	Beim Bearbeiten: Aktionen der Zeile (Inhalt leeren, Verdecken, Überschrift, Löschen …)

SCHNELLER ARBEITEN

Neuigkeiten

Kommt in Keyfiler etwas Neues dazu, erscheint nach der Anmeldung oben eine schmale Leiste: Neu in Keyfiler: … . Ansehen zeigt alle Neuigkeiten mit einer kurzen Erklärung und einem Link in die passende Hilfe; Ausblenden markiert sie als gelesen.

- **Jederzeit nachlesen:** im Kontomenü ⋯ unten in der Seitenleiste unter Neuigkeiten oder im Schnellzugriff.
- **Auf allen Geräten:** Was du einmal gelesen hast, erscheint auch auf deinen anderen Geräten nicht mehr als neu. Gemerkt wird dafür nur die zuletzt gesehene Versionsnummer.
- **Abschalten:** Einstellungen › Darstellung › Auf neue Funktionen hinweisen. Die Neuigkeiten im Kontomenü bleiben.

SCHNELLER ARBEITEN

Hell und dunkel

Keyfiler gibt es in einer hellen und einer dunklen Darstellung. Die dunkle schont abends die Augen und auf vielen Handys den Akku.

1. Öffne die Einstellungen über deinen Namen unten links und wähle Darstellung.
2. Wähle bei Erscheinungsbild: Wie das System, Hell oder Dunkel.

- **Wie das System:** voreingestellt. Keyfiler folgt der Einstellung von Windows, macOS, Android oder iOS – auch wenn dein Gerät abends automatisch umschaltet.
- **Schnell umschalten:** im Kontomenü ⋯ unten in der Seitenleiste mit dem Schalter bei Darstellung: Sonne für hell, halber Kreis für Wie das System, Mond für dunkel; das Menü schließt sich danach. Das klappt am Computer, Tablet und Handy gleich – praktisch, wenn der Bildschirm abends nicht wie eine Taschenlampe leuchten soll. Außerdem geht es im Schnellzugriff (Strg + K) mit Hell/Dunkel umschalten.
- **Pro Gerät:** Die Wahl gilt für dieses Gerät und diesen Browser. So kann das Handy dunkel sein und der PC im Büro hell. Gespeichert wird sie nur im Browser, nicht auf dem Server.
- **Inhalte farbig hervorheben:** Die Inhalte der Zeilen stehen in Dokumenten grün, damit sie sich von den Bezeichnungen abheben. Wer es lieber schlicht mag, schaltet das unter Einstellungen › Darstellung aus; dann stehen die Inhalte in der normalen Schriftfarbe. Die Wahl gilt für dein Konto auf allen Geräten.
- **Ausdrucke bleiben hell:** Drucken und die Druckvorschau sind immer schwarz auf weiß. PDFs und Bilder in der Vorschau stehen weiterhin auf weißem Grund.

Ton bei Hinweisen

Erscheint oben ein Hinweis – etwa zu einem Termin, zu Neuigkeiten, einer Freigabe oder einer Wartung –, spielt Keyfiler einen kurzen Ton, der Hinweis leuchtet kurz auf, und sein Symbol wackelt wie eine klingelnde Glocke – so siehst du, was den Ton ausgelöst hat. Mehrere Hinweise auf einmal ergeben nur einen Ton. Nach der Anmeldung erscheinen die Hinweise erst nach ein paar Sekunden, damit es nicht schon beim Öffnen klingelt. Ausschalten: Einstellungen › Darstellung › Ton bei Hinweisen; dort kannst du ihn auch Anhören. Wie das Erscheinungsbild gilt die Wahl nur für dieses Gerät. Aufleuchten und Wackeln gibt es auch ohne Ton; hast du am Gerät „Bewegung reduzieren“ eingestellt, bleibt das Symbol ruhig.

Am Handy: Bei mehreren Hinweisen siehst du zunächst nur den ersten, darunter 2 weitere Hinweise – ein Tipp darauf zeigt alle.

6 Sicherheit

SICHERHEIT

Sicherheits-Check

Wie gut bin ich geschützt? Der Sicherheits-Check zeigt auf einen Blick, was für die Sicherheit deines Kontos erledigt ist und was noch fehlt. Er läuft in deinem Browser – deine Kennwörter verlassen dabei nicht dein Gerät.

1. Öffne das Menü ⋯ neben deinem Benutzernamen unten links und wähle Sicherheits-Check.
2. Offene Punkte stehen oben, gelb markiert. Ein Klick auf den Knopf rechts führt direkt zur passenden Einstellung.

Was geprüft wird

- **Zwei-Faktor-Anmeldung:** ist sie eingerichtet? Siehe Zwei-Faktor-Anmeldung.
- **Wiederherstellungsschlüssel:** gibt es einen? Siehe Wiederherstellungsschlüssel.
- **Wiederherstellungscodes** (nur mit Zwei-Faktor-Anmeldung): sind noch genug übrig?
- **Kennwörter:** gibt es doppelt verwendete oder schwache? Details zeigt der Passwort-Check.
- **Sicherung:** ist eine fällig? Siehe Sicherung.

Der Balken oben hat ein Feld je Punkt: grün für erledigt, gelb für offen. Notfallblatt und Vorsorge stehen als Hinweise darunter und zählen nicht mit – ob du sie nutzt, entscheidest du.

> Ein kleiner gelber Punkt hinter dem Menüeintrag erinnert dich, solange Zwei-Faktor-Anmeldung oder Wiederherstellungsschlüssel fehlen oder eine Sicherung fällig ist.

SICHERHEIT

Passwort-Check

Der Passwort-Check prüft deine Kennwörter auf typische Schwachstellen. Er läuft in deinem Browser – der Server erfährt nichts davon. Auf Wunsch gleicht er sie zusätzlich mit bekannten Datenlecks ab.

1. Öffne das Menü ⋯ neben deinem Benutzernamen unten links und wähle Passwort-Check.
2. Wähle den Bereich: alle Tresore, einen Tresor oder einen Ordner. Ein Ordner wird mit allen Unterordnern geprüft.
3. Setze bei Bedarf das Häkchen Auch mit bekannten Datenlecks abgleichen (siehe unten). Es ist nie vorausgewählt.
4. Keyfiler zeigt das Ergebnis in Gruppen. Ein Klick auf einen Eintrag öffnet das Dokument. Mit Anderer Bereich … prüfst du weitere Bereiche.

Was die Ergebnisse bedeuten

- **In Datenlecks aufgetaucht** (nur mit Häkchen): Das Kennwort steht in Listen, die nach Hackerangriffen veröffentlicht wurden – Angreifer probieren solche Kennwörter zuerst. Keyfiler zeigt, wie oft es dort vorkommt. Ändere es beim jeweiligen Dienst, am besten sofort. PINs, TANs, Prüfnummern, Karten- und Kontonummern werden nicht abgeglichen.
- **Doppelt verwendet:** Dasselbe Kennwort steht in mehreren Dokumenten. Wird einer der Dienste gehackt, sind auch die anderen offen. Verglichen wird dabei mit allen Tresoren.
- **Schwach:** kürzer als 10 Zeichen, zu wenig Zufall oder mit bekanntem Muster, etwa gängigen Wörtern oder Tastaturfolgen. Keyfiler sagt dir jeweils, warum. PINs und TANs sind ausgenommen.

- **Lange nicht geändert:** seit über einem Jahr unverändert. Bei wichtigen Konten lohnt ein neues Kennwort.

So funktioniert der Abgleich mit Datenlecks

Keyfiler nutzt den Dienst Have I Been Pwned, der Milliarden Kennwörter aus bekannten Datenlecks sammelt. Dein Browser bildet aus jedem Kennwort eine Prüfsumme (SHA-1) und schickt nur deren erste 5 Zeichen. Der Dienst antwortet mit allen bekannten Prüfsummen, die so beginnen – meist einige Hundert, aufgefüllt mit Scheinwerten. Verglichen wird nur bei dir im Browser.

Weder deine Kennwörter noch ihre vollständigen Prüfsummen verlassen dein Gerät; der Dienst kann nicht erkennen, welches Kennwort gemeint war. Er sieht dabei aber deine IP-Adresse – deshalb fragt Keyfiler jedes Mal ausdrücklich. Details stehen in der Datenschutzerklärung.

So gehst du vor: Fang mit wichtigen Konten an – E-Mail, Bank, Shopping mit hinterlegter Zahlungsart. Erzeuge beim Dienst ein neues Kennwort mit dem Passwort-Generator und trage es in Keyfiler ein. Geprüft werden alle verdeckten Zeilen.

SICHERHEIT

Automatisches Sperren

Damit niemand an deine Daten kommt, wenn du deinen Platz verlässt, meldet Keyfiler dich automatisch ab. Danach brauchst du wieder dein Master-Passwort.

Die beiden Regeln

- **Sperren ohne Eingabe:** nach einer einstellbaren Zeit ohne Tastatur, Maus oder Berühren – von 1 bis 60 Minuten, voreingestellt 10 Minuten.
- **Sperren im Hintergrund:** wenn Keyfiler so lange in einem anderen Tab, Fenster oder hinter einer anderen App liegt – von 1 bis 30 Minuten, voreingestellt 2 Minuten.

Einstellen

1. Öffne die Einstellungen über deinen Namen unten links und wähle Konto.
2. Wähle bei Sperren ohne Eingabe und Sperren im Hintergrund die gewünschte Zeit oder schalte die Regel mit dem Schalter aus.

Schalte nicht beide Regeln aus. Dann sperrt Keyfiler nur noch, wenn du selbst sperrst, die Seite neu lädst oder nach spätestens 12 Stunden. Wer an dein entsperrtes Gerät kommt, sieht deine Kennwörter.

Sofort sperren

Klicke unten links auf das Schloss-Symbol neben deinem Benutzernamen oder drücke Strg + Umschalt + L (Mac: ⌘ + Umschalt + L). Keyfiler meldet dich sofort ab.

SICHERHEIT

So schützt Keyfiler deine Daten

Keyfiler arbeitet nach dem Zero-Knowledge-Prinzip: Alles wird in deinem Browser ver- und entschlüsselt. Der Server speichert nur verschlüsselte Daten und kann sie nicht lesen. Für Interessierte hier die Technik im Überblick.

Vom Master-Passwort zum Schlüssel

- Aus deinem Master-Passwort berechnet dein Browser mit **PBKDF2-SHA256 und 600.000 Durchläufen** einen Hauptschlüssel. Die vielen Durchläufe machen das Durchprobieren von Passwörtern sehr aufwendig.

- Aus dem Hauptschlüssel entstehen zwei getrennte Schlüssel: einer zum **Anmelden** – der Server bekommt nur einen davon abgeleiteten Wert und speichert ihn zusätzlich gehasht – und einer zum **Entschlüsseln**, der deinen Browser nie verlässt.
- Dein Master-Passwort selbst wird nie übertragen.

Verschlüsselung der Daten

- Jeder Tresor hat einen eigenen, zufälligen **AES-256-Schlüssel**. Damit werden Ordner, Dokumente – samt Namen – und Anhänge mit **AES-256-GCM** verschlüsselt. GCM erkennt zusätzlich, ob verschlüsselte Daten manipuliert wurden.
- Die Tresorschlüssel sind mit deinem persönlichen Kontoschlüssel verpackt, und dieser wiederum mit deinem Master-Passwort.
- Ein zweites Mal ist der Kontoschlüssel mit deinem Wiederherstellungsschlüssel verpackt. Deshalb funktioniert die Wiederherstellung, ohne dass jemand dein Passwort kennt.
- Außerdem hat jedes Konto ein **Schlüsselpaar (ECDH P-384)**. Der öffentliche Teil liegt offen auf dem Server, der private ist mit deinem Kontoschlüssel verpackt. Damit kann dir jemand bei einem gemeinsamen Tresor einen neuen Tresorschlüssel übergeben, den nur du öffnen kannst.
- Alles basiert auf der eingebauten Web-Crypto-Schnittstelle des Browsers, ohne Fremdbibliotheken.

Übertragung und Speicherort

- Die Verbindung ist zusätzlich mit TLS (https) geschützt.
- Die verschlüsselten Daten liegen auf Servern in Deutschland.
- Die Zwei-Faktor-Anmeldung schützt den Zugang zusätzlich; an der Verschlüsselung selbst ändert sie nichts.

> **Die Kehrseite:** Weil niemand außer dir die Schlüssel hat, kann auch niemand ein vergessenes Master-Passwort zurücksetzen. Bewahre deshalb deinen Wiederherstellungsschlüssel sorgfältig auf.

SICHERHEIT

Sicher unterwegs

Keyfiler funktioniert auf jedem Gerät mit Browser. Damit das auch unterwegs sicher bleibt, ein paar Regeln:

- **Fremde und öffentliche Computer meiden.** Auf Rechnern, die du nicht kennst, können Programme Tastatureingaben mitlesen. Nutze lieber dein eigenes Handy.
- **Wenn es doch sein muss:** Ein privates Browserfenster verwenden, nichts speichern lassen, geöffnete Anhänge löschen und dich am Ende mit dem Schloss unten links abmelden.
- **Öffentliches WLAN** ist durch die zusätzliche Verschlüsselung (https) unproblematisch. Achte trotzdem darauf, dass in der Adressleiste `keyfiler.com` steht.
- **Bildschirm im Blick:** Verdeckte Inhalte bleiben verdeckt, bis du sie aufdeckst. Kopierst du sie stattdessen, sieht sie niemand über deine Schulter.
- **Automatisches Sperren** eingeschaltet lassen – siehe Automatisches Sperren.
- **Gerät verloren?** Melde es unter `Einstellungen` › `Konto` › Angemeldete Geräte von einem anderen Gerät aus ab.

7 Sichern und Übertragen

SICHERN UND ÜBERTRAGEN

Backup erstellen und wiederherstellen

Deine Daten liegen verschlüsselt auf dem Server. Weil wir sie nicht lesen können, kann der Server auch keine lesbare Sicherung für dich anlegen. Eine eigene Sicherungsdatei schützt dich vor versehentlichem Löschen und ist deine Kopie, falls der Server einmal ausfällt.

Sicherung erstellen

1. Öffne die Einstellungen und wähle Datensicherung.
2. Klicke bei Sicherung erstellen auf Erstellen …
3. **Tresore:** Hake die Tresore an, die in die Sicherung sollen. Papierkorb, Kategorien und Vorlagen kommen immer mit.
4. **Passwort:** Vergib ein Sicherungspasswort (mindestens 12 Zeichen) und wiederhole es. Du kannst auch dein Master-Passwort verwenden. Klicke auf Sicherung herunterladen – Keyfiler speichert eine verschlüsselte Datei mit der Endung .keyfiler.
5. **Aufbewahren:** Keyfiler zeigt Dateiname und Inhalt der Sicherung und gibt Tipps, wo du sie aufbewahrst. Mit Fertig schließt du den Assistenten.

Abkürzung: Einen einzelnen Tresor sicherst du über ⋯ am Tresor › Diesen Tresor sichern … – dann beginnt der Assistent gleich beim Passwort. Im Schnellzugriff (Strg + K) findest du Sicherung erstellen und Aus Sicherung wiederherstellen.

Bewahre die Datei an einem sicheren Ort auf, am besten zusätzlich außerhalb deines Rechners, zum Beispiel auf einem USB-Stick oder einer externen Festplatte.

> **Ohne das Sicherungspasswort lässt sich die Datei nicht öffnen** – auch nicht von uns. Dafür ist sie unabhängig von deinem Konto: Sie funktioniert auch, wenn du dein Master-Passwort später änderst.

Erinnerung an die Sicherung

Unter Datensicherung stellst du bei An Sicherung erinnern ein, nach wie vielen Tagen Keyfiler dich erinnert – von 7 bis 90 Tagen oder nie. Voreingestellt sind 30 Tage. Ist deine letzte vollständige Sicherung aller Tresore älter, erscheint oben ein Hinweis mit Jetzt sichern …. Später blendet ihn für einen Tag aus.

Sicherung wiederherstellen

1. Öffne Einstellungen › Datensicherung und klicke bei Wiederherstellen auf Wiederherstellen … Alternativ: + neben Tresore › Aus Sicherung wiederherstellen …
2. Keyfiler führt dich in drei Schritten. **Datei:** Wähle die Sicherungsdatei, gib das Sicherungspasswort ein und klicke auf Weiter. Die Datei wird nur in deinem Browser entschlüsselt.
3. **Auswahl:** Wähle Einen Tresor, ganz oder teilweise, dann unter Tresor aus der Sicherung den Tresor, und hake im Baum an, was du zurückholen möchtest – einzelne Dokumente, ganze Ordner oder alles. Oder wähle Alle … Tresore komplett als neue Tresore, etwa nach einem Umzug – dann kommt auch der Papierkorb mit.
4. **Ziel:** Wähle unter Wiederherstellen in:
   - **einen neuen Tresor** – mit Name und Kategorie, oder
   - **einen vorhandenen Tresor** – mit Zielordner und auf Wunsch mit beibehaltener Ordnerstruktur.

5 Unter Außerdem kannst du Kategorien und Vorlagen aus der Sicherung ergänzen. Klicke dann auf Wiederherstellen.

Danach kannst du den Tresor öffnen oder mit Weiter wiederherstellen mehr aus derselben Sicherung holen – du landest wieder bei der Auswahl, ohne die Datei erneut zu öffnen.

Reicht der Platz deines Kontos nicht – zu viele Tresore oder zu wenig Speicher für die Anhänge –, sagt Keyfiler das schon im Schritt Ziel, bevor etwas wiederhergestellt wird.

Es wird nie etwas überschrieben. Gleichnamige Ordner werden zusammengeführt. Gibt es ein Dokument mit gleichem Namen schon, heißt das wiederhergestellte „… (Sicherung)“.

Lesbar exportieren (JSON oder CSV)

Möchtest du deine Daten in ein anderes Programm übernehmen, öffne Einstellungen › Datensicherung und klicke bei Lesbar exportieren auf Exportieren …. Wähle das Format, bestätige mit deinem Master-Passwort und klicke auf Exportieren.

- **JSON** enthält alles – Tresore, Ordner, Dokumente mit allen Zeilen und Bemerkungen, auf Wunsch auch die Anhänge.
- **CSV** ist eine Tabelle mit einer Zeile pro Feld, die sich direkt in Excel öffnen lässt. Anhänge stehen darin nur mit ihrem Namen.

Ein lesbarer Export ist nicht verschlüsselt. Alle Kennwörter stehen darin im Klartext. Lösche die Datei, sobald du sie nicht mehr brauchst. Für deine regelmäßige Sicherung nimm immer Sicherung erstellen.

SICHERN UND ÜBERTRAGEN

Daten aus der Desktop-Version übernehmen

Hast du bisher Keyfiler für Windows genutzt, übernimmst du deine Daten direkt in einen neuen Tresor. Die alten Dateien werden nur in deinem Browser gelesen und neu verschlüsselt; zum Server gelangt nur verschlüsselter Text.

Was du brauchst

- die Keyfiler-Datei mit der Endung .pkf,
- optional die zugehörige Anhang-Datei mit der Endung .pkfx,
- das Passwort, das du in der alten Keyfiler-Version verwendet hast.

So geht’s

1 Klicke in der Seitenleiste auf das + neben Tresore › Aus anderem Programm importieren … (oder Einstellungen › Datensicherung) und wähle in der Liste Keyfiler für Windows.

2 Wähle die .pkf-Datei und – falls vorhanden – die .pkfx-Datei mit den Anhängen, gib das Alte Keyfiler-Passwort ein und klicke auf Weiter.

3 Keyfiler zeigt, wie viele Einträge und Anhänge übernommen werden, und warnt, wenn Anhänge in der .pkfx-Datei fehlen.

4 Prüfe den Namen des neuen Tresors (er wird aus dem Dateinamen übernommen), wähle eine Kategorie und klicke auf … Einträge importieren.

Zum Schluss zeigt Keyfiler, wie viele Ordner, Dokumente und Anhänge übernommen wurden, und weist auf Einträge hin, die du prüfen solltest.

Bemerkungen prüfen

Die alte Version hat Zeilenumbrüche in Bemerkungen teilweise falsch gespeichert. Keyfiler listet nach dem Import die betroffenen Dokumente auf, in denen aus Zeilenumbrüchen Kommas geworden sein können. Sieh sie kurz durch und korrigiere sie bei Bedarf.

> **Lösche danach die alten Dateien sicher.** Die `.pkf`- und `.pkfx`-Dateien der alten Version sind nur schwach geschützt. Wenn alles übernommen ist, sollten sie nicht mehr herumliegen – auch nicht in Sicherungen oder im Papierkorb deines Rechners.

SICHERN UND ÜBERTRAGEN

Aus anderen Passwortmanagern importieren

Wechselst du von einem anderen Programm zu Keyfiler, nimmst du deine Einträge per Exportdatei mit – meist als CSV, aus 1Password, Bitwarden und KeePass auch vollständig mit Anhängen. Aus Keyfiler für Windows geht es über denselben Weg. Keyfiler liest die Datei nur in deinem Browser und verschlüsselt alles neu – zum Server gelangt nur das Chiffrat.

1. Aus dem alten Programm exportieren

- **Bitwarden:** Werkzeuge › Tresor exportieren › Format `.zip (mit Anhängen)` – ohne Anhänge genügt `.json` (siehe unten). Ein „verschlüsselter" Export lässt sich nicht lesen.
- **1Password:** Datei › Exportieren, Konto wählen, Format `1PUX`. Damit kommt alles mit (siehe unten). Das Format `CSV` enthält nur Logins und Passwörter ohne eigene Felder und Anhänge. Ältere Versionen bis 1Password 7 kennen kein 1PUX: Tresor wählen, Datei (Mac: Ablage) › Exportieren, Format `1PIF` (siehe unten).
- **LastPass:** Tresor im Browser › Erweiterte Optionen › `Exportieren`. Sichere Notizen kommen mit (siehe unten).
- **Apple Passwörter** (Mac): App `Passwörter` › Ablage › `Alle Passwörter in Datei exportieren`; bei älteren macOS-Versionen Safari › Ablage › Exportieren › `Passwörter`.
- **KeePass 2:** Datei › Exportieren › `KeePass XML (2.x)` – mit Gruppen und Anhängen (siehe unten). **KeePassXC:** Datenbank › Exportieren › `XML-Datei` – ohne Anhänge, die schreibt KeePassXC nicht hinein. CSV geht bei beiden auch, dann ohne eigene Felder.
- **Chrome und Edge:** Einstellungen › Passwörter (Passwortmanager) › Exportieren.
- **Firefox:** Passwörter (about:logins) › Menü `⋯` › Zugangsdaten exportieren.
- **Eigene Tabelle:** Eine Excel-Datei (`.xlsx`) oder LibreOffice-Tabelle (`.ods`) wählst du direkt über den Eintrag `Anderes Programm oder Tabelle` (Gruppe „Alles andere"); bei mehreren Blättern wählst du das Blatt. Titelzeilen über der Kopfzeile überspringt Keyfiler. Aus Numbers exportierst du nach Excel oder CSV.

2. In Keyfiler importieren

Wähle im Menü `+` bei `Tresore` oder unter `Einstellungen` › `Datensicherung` den Eintrag `Aus anderem Programm importieren`. Der Import führt dich in vier Schritten – oben siehst du, wo du bist, und kommst per Klick zu erledigten Schritten zurück:

1. **Programm:** Wähle, woher deine Daten kommen – auch `Keyfiler für Windows`.
2. **Datei:** Keyfiler zeigt kurz, wie du aus diesem Programm exportierst. Wähle die Datei oder zieh sie hinein – Keyfiler erkennt das Format am Inhalt.
3. **Auswahl:** Bei 1Password hakst du die Tresore an, bei Bitwarden entscheidest du über archivierte Einträge, bei Keyfiler für Windows und KeePass siehst du, was übernommen wird, bei einer eigenen Tabelle ordnest du die Spalten zu, sonst siehst du, was übernommen wird.
4. **Ziel:** Name und Kategorie des neuen Tresors. Mit `… Einträge importieren` geht es los.

Jeder Eintrag wird ein Dokument mit den Zeilen `Adresse`, `Benutzername`, `Kennwort` und – falls vorhanden – `2FA`; Notizen landen in den Bemerkungen, Ordner bzw. Gruppen bleiben erhalten. Zusätzliche Felder (z.B. aus Bitwarden) werden eigene Zeilen; Felder wie PIN oder CVC werden dabei verdeckt.

Vollständig aus 1Password (.1pux)

Wählst du eine `.1pux`-Datei, zeigt Keyfiler die 1Password-Tresore darin mit der Zahl der Einträge und Anhänge. Hake an, welche du übernehmen willst, und wähle:

- `Je 1Password-Tresor ein eigener Tresor` – mit gleichem Namen (gibt es den Namen schon, heißt der neue „… (1Password)“), oder
- `Alles in einen neuen Tresor` – jeder 1Password-Tresor wird darin ein Ordner.

Übernommen werden alle Arten von Einträgen – Logins, Kreditkarten, Bankkonten, Ausweise, Identitäten, sichere Notizen, Lizenzen, WLAN, Server und mehr. Abschnitte werden Überschriften, eigene Felder eigene Zeilen; verborgene Felder bleiben verdeckt, Datum, IBAN, BIC, Kartennummer und 2FA bekommen die passende Zeilenart. Das erste Tag wird zum Ordner, Notizen landen in den Bemerkungen, Dokumente und angehängte Dateien werden Anhänge. Archivierte Einträge übernimmst du auf Wunsch in einen Ordner `Archiv`. Den Verlauf alter Kennwörter übernimmt Keyfiler bewusst nicht.

> Reicht der Platz deines Kontos für die Tresore oder Anhänge nicht, sagt Keyfiler das vor dem Import – du kannst dann weniger Tresore wählen oder alles in einen Tresor übernehmen.

Ältere 1Password-Versionen (.1pif)

1Password 4 bis 7 exportieren im Format `1PIF`, und zwar einen Tresor nach dem anderen. Dabei entsteht ein Ordner mit der Datei `data.1pif` und – falls es Anhänge gibt – dem Ordner `attachments`. Einen Ordner kann der Browser nicht als Ganzes lesen, deshalb:

- **Mit Anhängen:** den Export-Ordner als ZIP komprimieren – am Mac Rechtsklick › `Komprimieren`, unter Windows Rechtsklick › `Senden an` › `ZIP-komprimierter Ordner` – und die ZIP-Datei wählen. Jeder Anhang kommt zum richtigen Eintrag.
- **Ohne Anhänge:** einfach die Datei `data.1pif` wählen.

Keyfiler übernimmt die Einträge wie beim 1PUX-Export – mit Abschnitten, eigenen Feldern, 2FA und den passenden Zeilenarten. Ordner aus 1Password bleiben Ordner; gibt es keine, wird das erste Tag zum Ordner. Einträge aus Papierkorb bzw. Archiv übernimmst du auf Wunsch in einen Ordner `Archiv`.

> Dokumente, die bei 1Password.com hochgeladen sind, schreibt 1Password nicht in den 1PIF-Export – die lädst du in 1Password einzeln herunter und hängst sie in Keyfiler an. Hast du mehrere Tresore, importierst du jeden Export einzeln. Und danach: Export-Ordner *und* ZIP löschen.

Vollständig aus Bitwarden (.zip oder .json)

Aus einer `.zip`- oder `.json`-Datei von Bitwarden übernimmt Keyfiler alle Einträge in einen neuen Tresor: Logins mit allen Adressen und 2FA, Karten, Identitäten, Bankkonten (IBAN und BIC), Führerscheine, Reisepässe, SSH-Schlüssel und sichere Notizen. Ordner und Sammlungen werden Ordner, eigene Felder eigene Zeilen unter `Weitere Felder`; verborgene Felder bleiben verdeckt. Anhänge enthält nur der ZIP-Export. Archivierte Einträge übernimmst du auf Wunsch in einen Ordner `Archiv`, gelöschte nie, den Verlauf alter Kennwörter bewusst nicht.

> Heißen mehrere Einträge gleich, legt Bitwarden ihre Anhänge nur nach der Reihenfolge ab. Keyfiler weist darauf hin – prüf nach dem Import kurz, ob die Dateien beim richtigen Eintrag sind.

LastPass: sichere Notizen

LastPass legt Kreditkarten, Bankkonten, Adressen, Ausweise, Versicherungen, WLAN, Server und Lizenzen als „sichere Notiz“ ab und schreibt deren Angaben als Text in die Exportdatei. Keyfiler teilt sie wieder in einzelne Zeilen auf – mit deutschen Bezeichnungen und der passenden Zeilenart: Kartennummer, IBAN und BIC, Geburts- und Ablaufdaten als Datum. PIN, Prüfnummer und Kennwörter bleiben verdeckt, der freie Text der Notiz landet in den Bemerkungen. Eigene Notizvorlagen werden mit ihren Feldnamen übernommen; Notizen ohne Vorlage bleiben Bemerkungen. Ordner bleiben erhalten, Anhänge enthält der CSV-Export von LastPass nicht.

Vollständig aus KeePass (.xml)

Aus der XML-Datei von KeePass oder KeePassXC übernimmt Keyfiler die Datenbank in einen neuen Tresor: Gruppen werden Ordner (ihre Notizen Bemerkungen), Einträge Dokumente mit `Adresse`, `Benutzername`, `Kennwort` und `2FA` – aus KeePassXC („otp“) wie aus KeePass („TimeOtp“). Eigene Felder werden eigene Zeilen unter `Weitere Felder`, geschützte Felder bleiben verdeckt, Schlagwörter kommen in eine Zeile. Läuft ein Eintrag ab, wird das Ablaufdatum eine Datumszeile `Gültig bis` und erscheint so bei den Fristen. Anhänge kommen mit, wenn sie in der Datei stehen (KeePass 2). Der Papierkorb und der Verlauf alter Kennwörter werden nicht übernommen.

Anderes Programm?

Erkennt Keyfiler das Programm (etwa „Bitwarden erkannt“), wird alles automatisch zugeordnet – du wählst nur noch den Namen des neuen Tresors.

Kennt Keyfiler das Format nicht, zum Beispiel bei einer selbst gepflegten Tabelle, steht unter `Was steht in welcher Spalte?` jede Spalte deiner Datei mit den ersten Werten als Beispiel. Rechts wählst du, was daraus wird: `Name des Dokuments`, `Adresse`, `Benutzername`, `Kennwort` usw., `als zusätzliche Zeile` oder `nicht übernehmen`. Vorschläge sind schon eingetragen – Keyfiler achtet dabei auf die Überschriften und auf den Inhalt (Webadressen, E-Mail-Adressen). Kennwörter bleiben in den Beispielen verdeckt.

> **Danach die Exportdatei löschen!** Ob CSV, Excel, .1pux, .1pif, .json, .zip oder .xml – sie enthält alle Passwörter lesbar. Lösch sie auch aus dem Papierkorb und dem Download-Ordner.

SICHERN UND ÜBERTRAGEN

Mehrere Geräte gleichzeitig nutzen

Du kannst Keyfiler auf beliebig vielen Geräten gleichzeitig verwenden – etwa am Rechner im Büro, am Laptop und auf dem Handy. Alle greifen auf dieselben Tresore zu.

So bleiben die Geräte abgeglichen

- Solange ein Tresor geöffnet und sichtbar ist, prüft Keyfiler alle 30 Sekunden und beim Zurückkehren in den Tab, ob sich etwas geändert hat. Neue Einträge erscheinen dann automatisch; deine Auswahl und aufgeklappte Ordner bleiben erhalten.
- Ein Dokument, das du gerade **bearbeitest**, wird nie einfach ersetzt. Wurde es inzwischen auf einem anderen Gerät geändert, erscheint ein Hinweis mit `Neu laden`.

Wenn beide Geräte dasselbe Dokument geändert haben

Speicherst du eine Fassung, die auf einem anderen Gerät schon geändert wurde, fragt Keyfiler nach, welche gelten soll. Mit `Meine Fassung speichern` setzt sich deine durch – die andere geht dabei verloren. Wurde das Dokument auf dem anderen Gerät sogar gelöscht, kannst du deine Änderungen `Als neues Dokument speichern`.

Abgeglichen werden nur verschlüsselte Daten. Der Server vergleicht dafür lediglich einen Fingerabdruck des Tresors, ohne Inhalte zu sehen.

8 Drucken und Dokumentieren

DRUCKEN UND DOKUMENTIEREN

Tresore und Ordner drucken

Keyfiler druckt alles von einem einzelnen Dokument bis zum ganzen Tresor in einem Durchgang – auf Papier oder als PDF.

1. Öffne den Tresor und drücke `Strg` + `P` oder wähle im Menü `⋯` eines Ordners oder Dokuments `Drucken …`
2. Keyfiler führt dich in Schritten. Kommst du aus einem Ordner oder Dokument, steht die Auswahl schon fest und du landest direkt beim letzten Schritt – ein Klick auf `Drucken` genügt.
3. **Auswahl:** Hake unter `Was soll gedruckt werden?` die Ordner und Dokumente an.
4. **Inhalt:** `Bemerkungen`, `Namen der Anhänge`, `verdeckte Inhalte im Klartext` (sonst stehen Kennwörter und PINs nicht auf dem Papier) und die Seitenaufteilung: `jedes Dokument auf eigener Seite` oder `fortlaufend (platzsparend)`.
5. **Titelseite:** `mit Titelseite` – mit Titel, `Für (optional)` und `Hinweis (optional)` – und `Inhaltsverzeichnis`. Beim Druck eines einzelnen Dokuments entfällt dieser Schritt.
6. **Drucken:** Kleine Seiten zeigen grob, wie Titelseite und die ersten Dokumente aussehen; darunter steht, was gedruckt wird – mit `ändern` springst du zum passenden Schritt. Werden Kennwörter lesbar gedruckt, ist das rot hervorgehoben. Klicke auf `Drucken`; im Druckdialog des Browsers wählst du einen Drucker oder `Als PDF speichern`.

Deine Einstellungen merkt sich das Gerät für den nächsten Ausdruck – außer Titel, Empfänger, Hinweis und „verdeckte Inhalte im Klartext“.

So sieht der Ausdruck aus: Die Inhalte – Kennwörter, IBAN, Codes und Bemerkungen – stehen in einer Schrift mit gleich breiten Zeichen, damit sich O und 0 oder I und 1 nicht verwechseln lassen. Titel und Bezeichnungen sind in der Schrift der App gesetzt. Ausdrucke sind immer hell, auch wenn du Keyfiler dunkel nutzt, und lassen sich auch schwarz-weiß gut lesen.

> **Ein Ausdruck oder PDF ist nicht verschlüsselt.** Mit „verdeckte Inhalte im Klartext“ stehen Kennwörter, PINs und 2FA-Schlüssel lesbar darin. Bewahre ihn entsprechend sicher auf und lösche PDFs, die du nicht mehr brauchst.

DRUCKEN UND DOKUMENTIEREN

Dokumentation für Kunden

Betreust du Websites, Server oder Netzwerke für Kunden, wird Keyfiler zu deiner IT-Dokumentation – und am Projektende übergibst du sie mit wenigen Klicks.

Gut organisiert

- **Ein Ordner oder Tresor pro Kunde:** Für wenige Kunden genügt ein Tresor „Kunden“ mit einem Ordner je Kunde. Viele oder große Kunden bekommen besser einen eigenen Tresor – das hält die Daten sauber getrennt.
- **Vorlagen nutzen:** Lege Dokumentvorlagen für wiederkehrende Einträge an, etwa Webhosting, Domain & DNS, Datenbank oder WordPress-Admin. So sind alle Dokumentationen gleich aufgebaut.
- **Überschriften und Bemerkungen:** Gliedere Dokumente mit Überschriften und halte Besonderheiten in den Bemerkungen fest.

Übergabe als Dokumentation

1. Wähle den Ordner oder Tresor des Kunden und öffne `Drucken …`
2. Aktiviere `mit Titelseite`, trage bei `Für (optional)` den Kunden ein und ergänze bei Bedarf einen Hinweis.

3. Schalte Inhaltsverzeichnis und verdeckte Inhalte im Klartext ein – der Kunde braucht die Zugangsdaten ja.
4. Speichere das Ergebnis im Druckdialog als PDF.

Sicher übergeben: Das PDF ist unverschlüsselt. Schicke es nicht per normaler E-Mail, sondern übergib es persönlich, auf Papier oder über einen verschlüsselten Weg – und lösche deine Kopie danach.

9 Konto

KONTO

E-Mail-Adresse ändern

Deine E-Mail-Adresse ist dein Benutzer für die Anmeldung. Du kannst sie jederzeit ändern; dein Master-Passwort, deine Tresore und dein Wiederherstellungsschlüssel bleiben dabei unverändert.

1. Öffne Einstellungen › Konto und klicke bei E-Mail-Adresse auf Ändern …
2. Gib die neue E-Mail-Adresse und zur Bestätigung dein Master-Passwort ein.
3. Klicke auf Ändern. Ab sofort meldest du dich mit der neuen Adresse an.

Andere Geräte: Dort meldet dich Keyfiler nach der Änderung ab. Melde dich einfach mit der neuen Adresse wieder an.

KONTO

Master-Passwort ändern

1. Öffne Einstellungen › Konto und klicke bei Master-Passwort auf Ändern …
2. Gib dein Bisheriges Passwort ein, dann zweimal das Neue Passwort.
3. Bestätige. Das neue Master-Passwort gilt ab sofort.

Deine anderen Geräte werden dabei abgemeldet und brauchen das neue Passwort. Dein Wiederherstellungsschlüssel und vorhandene Sicherungsdateien bleiben gültig.

Ein gutes Master-Passwort

- **Lang statt kompliziert:** mindestens 12 Zeichen, besser 14 oder mehr. Ein Satz aus mehreren Wörtern lässt sich gut merken und ist trotzdem stark.
- **Einzigartig:** Verwende es nirgendwo sonst.
- **Nur in deinem Kopf** – und als Notfall-Lösung gibt es den Wiederherstellungsschlüssel.

KONTO

Angemeldete Geräte

Unter Einstellungen › Konto › Angemeldete Geräte siehst du, in welchen Browsern und auf welchen Geräten du gerade angemeldet bist – etwa „Firefox auf Windows“ oder „Safari auf iPhone“, mit dem Zeitpunkt der Anmeldung und der letzten Aktivität. Das Gerät, an dem du gerade arbeitest, ist mit (dieses Gerät) markiert.

- **Ein Gerät abmelden:** Abmelden in seiner Zeile. Die Anmeldung dort endet sofort.
- **Alle anderen abmelden:** unten im Dialog. Das Gerät, an dem du gerade arbeitest, bleibt angemeldet.
- Abmelden, Sperren und das automatische Sperren beenden eine Anmeldung ebenfalls; sie verschwindet dann aus der Liste.

Gespeichert wird dafür nur eine grobe Bezeichnung aus dem Browser – keine IP-Adresse und kein Ort. Beendete Anmeldungen löscht Keyfiler nach einem Tag.

E-Mail bei neuem Gerät

Meldet sich jemand mit einem Browser an, den Keyfiler für dein Konto noch nicht kennt, bekommst du eine E-Mail mit der Bezeichnung des Geräts und dem Zeitpunkt – mit Master-Passwort, Passkey, Zwei-Faktor-Anmeldung oder Wiederherstellungsschlüssel. So merkst du sofort, wenn jemand anderes deine Zugangsdaten benutzt.

- **Erkennen:** Nach der Anmeldung merkt sich der Browser ein zufälliges Cookie. Keyfiler speichert davon nur einen Prüfwert und die grobe Bezeichnung – keine IP-Adresse, keinen Ort.
- **Keine E-Mail** bei der allerersten Anmeldung eines Kontos und bei der ersten Anmeldung nach Einführung der Funktion.
- **Bekannte Geräte:** Unter Einstellungen › Konto › Bekannte Geräte siehst du alle Browser, die Keyfiler kennt, und kannst einzelne vergessen. Nach 12 Monaten ohne Anmeldung vergisst Keyfiler ein Gerät von selbst.
- **Abschalten:** Einstellungen › Konto › E-Mail bei neuem Gerät.
- Löschst du die Cookies deines Browsers oder arbeitest du in einem privaten Fenster, gilt jede Anmeldung als neues Gerät.

Ein Gerät, das du nicht kennst? Melde es ab, ändere dein Master-Passwort und richte die Zwei-Faktor-Anmeldung ein, falls noch nicht geschehen.

KONTO

Feedback senden

Wünsche, Kritik, einen Fehler, eine Frage oder Lob schickst du direkt aus der App: Kontomenü unten links → Feedback … oder im Schnellzugriff (Strg + K) Feedback senden.

1. Wähle, worum es geht, und schreib deine Nachricht (bis 2000 Zeichen).
2. Lass Version und Browser mitschicken eingeschaltet, wenn es um einen Fehler geht – mitgeschickt wird nur eine grobe Angabe wie „Firefox auf Windows“.
3. Gibt es Einträge im Fehlerprotokoll, kannst du es mit Fehlerprotokoll mitschicken anhängen – bei „Fehler“ ist das Häkchen schon gesetzt. Das hilft uns sehr, ein Problem nachzuvollziehen.
4. Senden. Antworten kommen per E-Mail an deine Adresse.

Keine Kennwörter oder vertraulichen Inhalte. Anders als deine Tresore ist Feedback nicht verschlüsselt – der Administrator liest es so, wie du es geschrieben hast.

KONTO

Konto löschen

Du kannst dein Konto jederzeit selbst löschen. Dabei werden alle Tresore, Dokumente und Anhänge vom Server entfernt. Nur die Einträge im Protokoll der E-Mails und Vorgänge bleiben als Nachweis erhalten – 3 Jahre ab Ende des Jahres, mit Benutzernamen und Zeitpunkten, ohne Inhalte.

Das lässt sich nicht rückgängig machen. Lade vorher eine Sicherung herunter, wenn du deine Daten behalten möchtest.

1. Öffne Einstellungen › Konto.
2. Klicke ganz unten bei Konto löschen auf Löschen …
3. Bestätige mit Konto endgültig löschen.

Danach bist du abgemeldet, und dein Konto existiert nicht mehr. Fragen zur Löschung oder zu gespeicherten Daten beantworten wir unter info@keyfiler.com.

KONTO

Protokoll

Keyfiler hält fest, was als Nachweis nötig ist – so wenig wie möglich, so viel wie nötig: welche E-Mails es verschickt hat, wer wann Zugriff auf einen gemeinsamen Tresor oder einen Vorsorgeordner bekommen oder verloren hat, Änderungen am Konto (angelegt, gelöscht, Zustimmung zu den Nutzungsbedingungen, Master-Passwort, E-Mail-Adresse, Zwei-Faktor) und Eingriffe von Admins. Inhalte, Tresornamen, Schlüssel und Codes stehen nie darin.

Nicht im Protokoll stehen Vorgänge ohne Nachweiszweck – etwa erstellte oder zurückgezogene Einladungen (belegt ist die E-Mail bzw. später der Beitritt), deine eigene Auskunft über gespeicherte Daten, geänderte E-Mail-Vorlagen (deren Fassungen speichern das selbst) und Mitteilungen an alle samt den E-Mails dazu.

Deine eigenen Einträge

Unter Einstellungen › Protokoll siehst du die E-Mails an dich und die Vorgänge, die du ausgelöst hast oder die dich betreffen. Wähle Art und Zeitraum und klicke auf Anzeigen …: Die Treffer erscheinen in einem Fenster, nach Tagen geordnet und je 50 auf einmal (Weitere laden). Ein Klick auf einen Eintrag klappt ihn auf – bei E-Mails mit dem Text, wie er verschickt wurde. Diesen Eintrag ausdrucken oder als PDF speichern liefert einen Nachweis, Treffer ausdrucken die ganze Liste (ohne E-Mail-Texte).

- „Vom E-Mail-Server angenommen“ belegt, dass Keyfiler die E-Mail verschickt hat – nicht, dass sie im Postfach angekommen ist. Das kann kein Absender feststellen.
- Einträge lassen sich nicht ändern: Was verschickt ist, ist verschickt. Sie bleiben 3 Jahre ab Ende des Jahres erhalten – ein Eintrag aus 2026 also bis zum 31.12.2029 –, auch wenn ein Konto gelöscht wird. So lange können Ansprüche geltend gemacht werden (regelmäßige Verjährung).

Was ist über mich gespeichert?

Unter Einstellungen › Konto › Gespeicherte Angaben stellt Keyfiler zum Ausdrucken oder als PDF zusammen, was der Server über dein Konto weiß: Kontodaten, Umfang deiner verschlüsselten Daten, gemeinsame Tresore, Notfallzugänge, Anmeldeversuche und alle Protokolleinträge (Auskunft nach Art. 15 DSGVO). Die Inhalte selbst kann der Server nicht lesen – die sicherst du unter Datensicherung.

KONTO

Fehlerprotokoll

Geht in der App etwas schief, hält Keyfiler das fest: Zeitpunkt, welche Aktion betroffen war, HTTP-Status, Fehlercode und die Meldung, die du gesehen hast – die letzten 50 Fehler, gleiche kurz hintereinander zusammengefasst. Inhalte stehen nie darin: keine Namen von Tresoren oder Einträgen, keine Kennwörter, keine Dateinamen.

- Normalerweise steht das Protokoll nur im Arbeitsspeicher, solange Keyfiler geöffnet ist – nach dem Neuladen ist es leer. Mit Auf diesem Gerät aufbewahren bleibt es im Browser erhalten; das ist sinnvoll, wenn wir einem Fehler gemeinsam nachgehen. Ausschalten löscht es wieder.
- Unter Einstellungen › Protokoll › Fehlerprotokoll zeigt Anzeigen … die Einträge, Kopieren legt sie als Text in die Zwischenablage, Leeren löscht sie.
- An uns geht das Protokoll nur, wenn du es beim Feedback ausdrücklich mitschickst.

10 Fehler und Probleme

FEHLER UND PROBLEME

Ich kann mich nicht anmelden

Die häufigsten Ursachen lassen sich schnell selbst beheben.

Das Master-Passwort wird nicht akzeptiert

- **Eingabe ansehen:** Das Auge rechts im Feld (oder Alt + F8) zeigt, was du getippt hast. Achte darauf, dass niemand mitliest. Das gilt in allen Passwortfeldern von Keyfiler.
- **Feststelltaste:** Ist die Großschreibung aktiviert?
- **Tastaturbelegung:** Auf einem fremden Gerät kann eine andere Belegung aktiv sein, etwa Englisch, wo Y und Z vertauscht sind und Sonderzeichen woanders liegen.
- **Benutzer prüfen:** Stimmt die E-Mail-Adresse im Feld Benutzer?
- **Passwort wirklich vergessen?** Dann hilft dein Wiederherstellungsschlüssel – siehe Wiederherstellungsschlüssel.

„Zu viele Fehlversuche“

Nach mehreren falschen Eingaben sperrt Keyfiler weitere Versuche für einige Minuten – zum Schutz vor Angreifern, die Passwörter durchprobieren. Die Meldung sagt dir, wann du es erneut versuchen kannst.

Der Zwei-Faktor-Code wird abgelehnt

- **Uhrzeit des Handys:** Die Codes hängen von der genauen Uhrzeit ab. Stelle Datum und Uhrzeit am Handy auf „automatisch“.
- **Richtiger Eintrag:** Nimm den Code aus dem Eintrag „Keyfiler“ in deiner Authenticator-App.
- **Code abgelaufen:** Ein Code gilt nur 30 Sekunden. Warte auf den nächsten und gib ihn zügig ein.
- **Handy nicht zur Hand?** Wähle Wiederherstellungscode verwenden – siehe Zwei-Faktor-Anmeldung.

Der Passkey klappt nicht

- **Fenster geschlossen oder zu lange gewartet:** Klicke auf Mit Passkey bestätigen und versuch es noch einmal.
- **Anderes Gerät:** Ein Passkey liegt auf dem Gerät, auf dem du ihn eingerichtet hast (bzw. in deinem Apple-, Google- oder Microsoft-Konto). An einem fremden PC wählst du im Fenster deines Geräts das Handy per QR-Code – oder nimmst Code bzw. Wiederherstellungscode.
- **Andere Adresse:** Passkeys gelten nur unter keyfiler.com. Rufst du die App über eine andere Adresse auf, findet dein Gerät keinen passenden Passkey.

„Du wurdest automatisch abgemeldet“

Das ist gewollt: Keyfiler meldet dich ab, wenn du eine Weile nichts eingibst oder die App im Hintergrund liegt. Wie lange das dauert, stellst du selbst ein – siehe Automatisches Sperren.

Wartung oder abgelaufener Testzugang

Während einer angekündigten Wartung ist die Anmeldung kurz nicht möglich; die Meldung nennt das voraussichtliche Ende. Bei einem Testzugang ist nach dessen Ablauf keine Anmeldung mehr möglich – melde dich in diesem Fall bei uns.

Die Seite lädt nicht oder sieht fehlerhaft aus

- Lade die Seite neu – am Computer mit Strg + Umschalt + R, am Mac mit ⌘ + Umschalt + R.
- Bei der installierten App: App schließen und neu öffnen.
- Prüfe, ob du einen aktuellen Browser verwendest.

Nichts hilft?

Schreib uns an info@keyfiler.com und beschreibe, was du tust und was passiert – gern mit Browser, Gerät und einem Screenshot der Meldung.

> **Schicke uns niemals dein Master-Passwort, deinen Wiederherstellungsschlüssel, Wiederherstellungscodes oder Zwei-Faktor-Codes.** Wir fragen nie danach – auch nicht per E-Mail oder Telefon.

FEHLER UND PROBLEME

Die App zeigt eine alte Version

Keyfiler wird laufend weiterentwickelt. Damit die App schnell startet, legt dein Browser ihre Programmdateien ab – bei jedem Aufruf fragt Keyfiler aber zuerst beim Server nach der aktuellen Version und lädt bei einer neuen die geänderten Dateien neu. Sollte trotzdem einmal eine alte Fassung erscheinen, helfen diese Schritte. Welche Version du gerade nutzt, siehst du unter Einstellungen › Über Keyfiler. Kleines Detail am Rande: Der Tresor dort öffnet sich mit der Versionsnummer als Kombination – bei Version 0.81.0 rechts auf 0, links auf 81, rechts auf 0. Ein Klick auf den Tresor spielt das noch einmal ab.

So holst du die aktuelle Version

- **Neu laden ohne Zwischenspeicher:** Strg + Umschalt + R, am Mac ⌘ + Umschalt + R.
- **Installierte App:** Schließe die App vollständig und öffne sie neu. Auf dem Handy: aus der App-Übersicht wegwischen und neu starten.
- **Hilft das nicht:** Lösche in den Browser-Einstellungen die gespeicherten Daten für keyfiler.com. Deine Tresore sind davon nicht betroffen – sie liegen verschlüsselt auf dem Server. Du musst dich danach nur neu anmelden.

FEHLER UND PROBLEME

Unterstützte Browser und Geräte

Keyfiler läuft in jedem aktuellen Browser – auf Computer, Tablet und Handy. Du brauchst nichts zu installieren. Wenn du möchtest, kannst du Keyfiler aber als App installieren.

Browser

- **Google Chrome und Microsoft Edge** ab Version 111
- **Mozilla Firefox** ab Version 121
- **Apple Safari** ab Version 16.4 (Mac, iPhone und iPad)
- **Andere Browser** auf Basis von Chrome, etwa Samsung Internet, Opera oder Brave, in einer aktuellen Version

Am besten nutzt du immer die neueste Version deines Browsers. Updates schließen auch Sicherheitslücken.

Geräte

- **Computer:** Windows, macOS und Linux.
- **Android:** Handy und Tablet mit einem aktuellen Chrome.
- **iPhone und iPad:** ab iOS bzw. iPadOS 16.4. Auf diesen Geräten nutzen alle Browser die Technik von Safari, deshalb zählt hier die Version des Betriebssystems.

Nicht unterstützt

- **Internet Explorer** und andere veraltete Browser.
- **Browser, die JavaScript abschalten.** Keyfiler verschlüsselt deine Daten mit JavaScript direkt im Browser und funktioniert ohne nicht.

Privates Fenster: Keyfiler funktioniert auch im privaten bzw. Inkognito-Fenster. Das ist praktisch auf fremden Geräten – siehe Sicher unterwegs.

FEHLER UND PROBLEME

Kontakt bei Problemen

Findest du hier keine Lösung, schreib uns an info@keyfiler.com. Damit wir schnell helfen können, nenne bitte:

- was du tun wolltest und was stattdessen passiert ist,
- den genauen Wortlaut einer Fehlermeldung – gern als Screenshot,
- Gerät, Betriebssystem und Browser (zum Beispiel „Windows 11, Chrome“),
- die Keyfiler-Version aus `Einstellungen` › `Über Keyfiler`.

> **Schicke uns niemals dein Master-Passwort, deinen Wiederherstellungsschlüssel, Wiederherstellungscodes oder Zwei-Faktor-Codes.** Wir fragen nie danach. Achte auch bei Screenshots darauf, dass keine Kennwörter zu sehen sind.