



Passwortmanager- Handout

Ihr digitaler Schlüsselbund für den Arbeitsalltag – einfach und sicher.



Erste Schritte vor der Nutzung eines Passwortmanagers

Kurzfassung:

- ✓ Entfernen Sie alte Passwort-Zettel, Notizen und Fotos
- ✓ Prüfen und ordnen Sie Ihre bestehenden Passwörter
- ✓ Tragen Sie alle Logins in den Passwortmanager ein
- ✓ Löschen Sie unsichere oder doppelt gespeicherte Listen
- ✓ Organisieren Sie gemeinsame Zugänge über Team-Tresore
- ✓ Notieren Sie Ihr Master-Passwort sicher im Notfall-Kit

▼ Ausführlichere Anleitung

1. Aufräumen: Unsichere Passwort-Speicher entfernen

- Entfernen Sie **Zettel und Notizen** mit Passwörtern von Monitoren, Schreibtischen, Pinnwänden oder Schubladen.

👉 Diese Daten gehören künftig ausschließlich in den Passwortmanager.

- Löschen Sie **Fotos oder Screenshots** von Passwörtern auf Smartphones oder Computern.
- Durchsuchen und löschen Sie **WhatsApp-Nachrichten oder E-Mails**, in denen Passwörter enthalten sind.

(Tipp: In WhatsApp mit der Suchfunktion „Passwort“ eingeben.)

2. Bestehende Passwortlisten systematisch erfassen

- Öffnen Sie Ihre bisherige **Excel-Tabelle, Notiz oder Ihr Heft** mit Passwörtern.
- Gehen Sie Zeile für Zeile durch und entscheiden Sie:
 - Welche Passwörter sind **noch aktuell**?
 - Welche können **gelöscht oder ersetzt** werden?
- Diese bereinigte Liste dient als Grundlage, um alle Passwörter in den Manager zu übertragen.

3. Passwörter sicher übertragen

- Öffnen Sie den Passwortmanager (z. B. *1Password*).
 - Für jeden Eintrag aus Ihrer Liste:
 1. Neues Login im Passwortmanager anlegen
 2. Benutzernamen, Website und Passwort eintragen
 3. Falls das Passwort schwach ist → **ein neues, starkes Passwort generieren**
 - Sobald alle Daten übertragen sind:
 - ✗ **Löschen Sie die Excel-Datei oder das Dokument dauerhaft.**
- So vermeiden Sie doppelte, unsichere Speicherorte.

4. Gemeinsame Zugänge richtig ablegen

- Legen Sie für **gemeinsam genutzte Logins** (z. B. für Bestellportale, Social Media oder WLAN) einen **geteilten Tresor** im Passwortmanager an.

- Teilen Sie Passwörter **nicht mehr über Zettel, WhatsApp oder E-Mail**, sondern ausschließlich über den Passwortmanager.
- Jeder Mitarbeitende sollte einen eigenen Zugang zum Passwortmanager erhalten – **keine gemeinsamen Logins**.

5. Backup & Notfall-Absicherung

- Schreiben Sie Ihr **Master-Passwort** in das **Notfall-Kit** (eine vorbereitete Karte oder PDF) und bewahren Sie es sicher auf.
- Aktivieren Sie, wenn möglich, die **biometrische Entsperrung** (Fingerabdruck oder Gesichtserkennung), um den Alltag zu erleichtern.
- Prüfen Sie, ob ein **Administrator oder Verantwortlicher** im Betrieb im Notfall eine **Wiederherstellung** Ihres Kontos veranlassen kann.



Was ist 1Password?



Stellen Sie sich 1Password wie einen hochsicheren digitalen Safe (Tresor) für all Ihre Passwörter und wichtigen Daten vor. Sie müssen sich nur noch **EIN einziges Passwort merken** – den Rest erledigt 1Password für Sie. Die Software kann starke Passwörter für Sie generieren, Login-Formulare automatisch ausfüllen und synchronisiert Ihre Daten geräteübergreifend (Computer & Smartphone). Zudem können Sie darin Kreditkarteninformationen und vertrauliche Notizen sicher speichern, um alle wichtigen Daten zentral und verschlüsselt an einem Ort aufzubewahren. Auch das sichere Teilen von Passwörtern im Team wird unterstützt.

Ähnliche Tools, die auf vergleichbare Weise arbeiten, sind **LastPass**, **Dashlane**, **Bitwarden**, **Keeper** und **NordPass**. Es gibt zahlreiche weitere Anbieter auf dem Markt – **1Password dient hier als beispielhafte Beschreibung** für diese Art von Passwort- und Datensicherheitslösungen.



Installation und Einrichtung



1. Download & Installation (Computer)

Laden Sie 1Password von der [offiziellen Webseite](#) herunter und installieren Sie das Programm. Folgen Sie dann dem Einladungslink Ihrer Firma per E-Mail, um sich mit Ihrem Firmenkonto anzumelden.

2. Das Master-Passwort festlegen

Legen Sie ein starkes Master-Passwort fest. Dieses Passwort schützt alle Ihre Daten – wählen Sie also etwas Einzigartiges, das Sie sich gut merken können (z.B. eine Kombination aus mehreren Wörtern und mind. einem Sonderzeichen wie `MeinLieblingshammerIstVon1998!`).

WICHTIG: Notfall-Kit ausdrucken!

Nach der Einrichtung erhalten Sie ein PDF ("Notfall-Kit"). ****DRUCKEN SIE DIESES DOKUMENT AUS!**** Es enthält Ihren Geheimschlüssel, den Sie für die Anmeldung auf neuen Geräten benötigen. ****Schreiben Sie auch Ihr Master-Passwort handschriftlich auf diesen Ausdruck.**** Bewahren Sie es an einem sicheren Ort auf.

3. Browser-Erweiterung installieren

Installieren Sie die 1Password Browser-Erweiterung für Ihren Webbrowser. Diese Erweiterung ermöglicht das automatische Speichern und Ausfüllen von Passwörtern direkt im Browser und ist der Schlüssel zum komfortablen Arbeiten.

- [1Password für Google Chrome](#)
- [1Password für Mozilla Firefox](#)
- [1Password für Microsoft Edge](#)

4. Schneller entsperren mit Biometrie

Sie können in den Einstellungen auch die biometrische Entsperrung aktivieren (z.B. Fingerabdruck/Windows Hello oder Gesichtserkennung/FaceID). Dann genügt Ihr Fingerabdruck, um 1Password schnell und sicher zu entsperren.

5. Einrichtung auf dem Smartphone (Optional)

Installieren Sie die 1Password-App aus dem App Store (iPhone) oder Google Play Store (Android). Melden Sie sich mit Ihrem Konto an (am einfachsten geht das durch Scannen des QR-Codes aus Ihrem Notfall-Kit). Aktivieren Sie die Autofill-Funktion, damit 1Password auch in mobilen Browsern und Apps Passwörter automatisch eingeben kann.

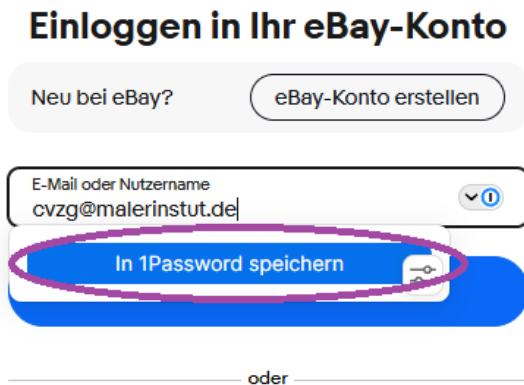
- 1Password im Apple App Store (für iPhone/iPad).
- 1Password im Google Play Store (für Android).

Anlegen, Speichern & Nutzen von Passwörtern

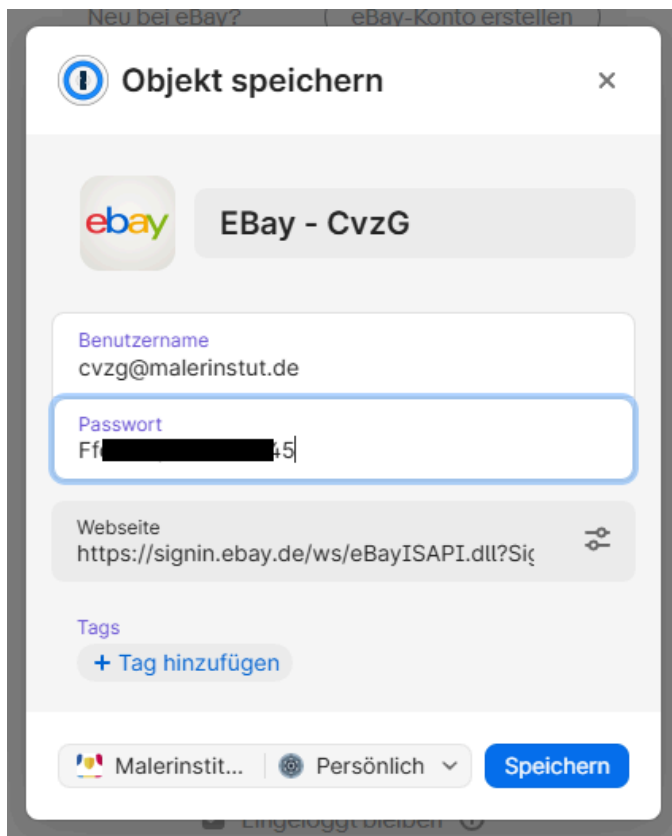


Automatisch beim Einloggen speichern

Jedes Mal, wenn Sie sich auf einer Webseite anmelden oder ein neues Konto erstellen, erkennt 1Password dies. Nachdem Sie Benutzername und Passwort eingegeben haben, bietet 1Password an, die Zugangsdaten zu speichern. Klicken Sie einfach auf ****„In 1Password speichern“****.



The screenshot shows the eBay login interface. At the top, it says "Einloggen in Ihr eBay-Konto". Below this are two links: "Neu bei eBay?" and "eBay-Konto erstellen". The main login form has a text input field labeled "E-Mail oder Nutzername" containing the email "cvzg@malerinstitut.de". To the right of the input field is a dropdown menu with a checkmark and an information icon. Below the input field, a blue button with the text "In 1Password speichern" and a key icon is highlighted with a red oval. At the bottom of the form, there is a horizontal line with the word "oder" in the center.

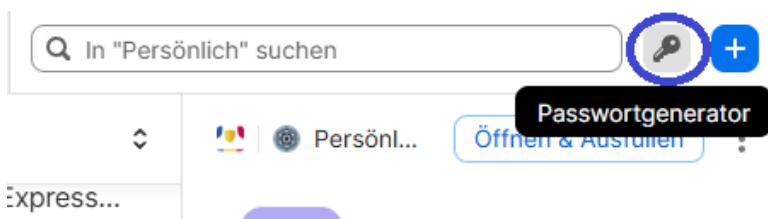


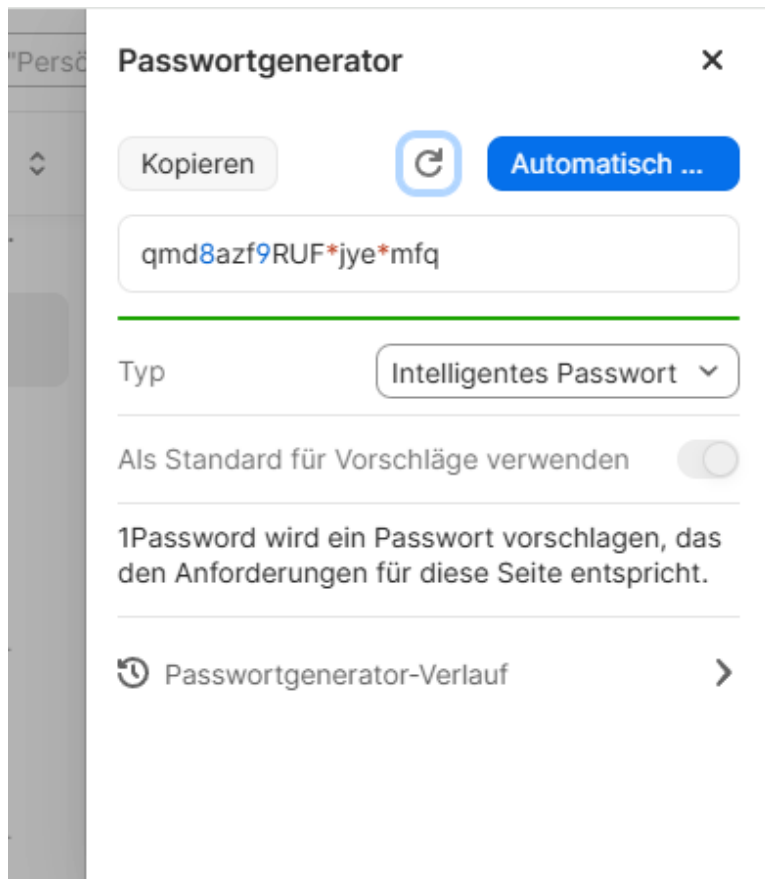
Manuell in der App hinzufügen

Sie können Passwörter auch direkt in der 1Password-App erfassen. Öffnen Sie die App, klicken Sie auf „Neu“ und wählen Sie die Kategorie „Login“. Tragen Sie alle Daten ein und speichern Sie den Eintrag.

Starke Passwörter mit dem Generator erstellen

Wenn Sie ein neues Konto erstellen oder ein Passwort ändern, schlägt 1Password automatisch ein sicheres, zufälliges Passwort vor. Klicken Sie im Passwort-Eingabefeld auf das 1Password-Symbol und wählen Sie ****„Vorgeschlagenes Passwort verwenden“****. Sie brauchen sich dieses Passwort nicht zu merken – es wird sicher in 1Password gespeichert.





Automatisches Ausfüllen in Webbrowsern

Gehen Sie auf eine Webseite, bei der Sie sich anmelden möchten. In den Eingabefeldern erscheint ein kleines 1Password-Icon. Klicken Sie darauf und wählen Sie den entsprechenden Konto-Eintrag aus. 1Password füllt nun automatisch Benutzername und Passwort in die Formularfelder ein.

Log in

Email

Pipedrive
cvzg@malerinstitut.de

Password

[Forgot?](#)

Log in

☐ Remember me

or access quickly

Google SSO

[Don't have an account?](#)

[Having issues logging in?](#)

Gemeinsame Nutzung von Tresoren im Team



In 1Password sind Tresore vergleichbar mit Ordnern, in denen Passwörter abgelegt werden.

- **Privater Tresor:** Den sehen nur Sie. Ideal für persönliche Zugänge wie Ihr E-Mail-Passwort.
- **Gemeinsame Tresore:** Auf diese haben mehrere berechtigte Personen Zugriff. Ihr Unternehmen kann z.B. einen Tresor für das Team oder eine Abteilung einrichten, in dem alle gemeinsamen Passwörter liegen (z.B. WLAN-Passwort, Zugänge für Lieferantenportale etc.).

Passwort mit Kollegen teilen

Wenn Sie ein Login aus Ihrem privaten Tresor mit einem Kollegen teilen möchten, verschieben oder kopieren Sie den Eintrag einfach in einen geteilten

Tresor. Jeder, der Zugriff auf diesen Tresor hat, kann den Eintrag dann sehen und verwenden.

Tipp: Das Verwalten, Verschieben und Ändern von Einträgen ist oft am einfachsten direkt in der Web-Oberfläche von 1Password unter:

<https://my.1password.eu/home>.

Kosten und Pläne



1Password ist ein abonnementbasierter Dienst. Für Unternehmen sind in der Regel die "Teams"- oder "Business"-Pläne relevant. Hier eine kurze Übersicht:

Individual	Families	Starterpaket für Teams	Business
Übernimm die Kontrolle über deine Online-Sicherheit.	Sorgenfreiheit für deine ganze Familie.	Schütze dein kleines Team.	Sicherheit, die sich an dein Unternehmen anpasst.
€2.65 EUR pro Monat. Jährliche Abrechnung.	€4.75 EUR pro Monat. Jährliche Abrechnung.	€16.95 EUR Bis zu 10 Nutzer/Monat. Jährliche Abrechnung.	€6.99 EUR pro Nutzer, pro Monat. Jährliche Abrechnung.
14 Tage KOSTENLOS testen	14 Tage KOSTENLOS testen	14 Tage KOSTENLOS testen	14 Tage KOSTENLOS testen
• Passwörter sicher generieren • Zugangsdaten automatisch speichern und ausfüllen von Zugangsdaten • Elemente sicher mit allen teilen • Verwendung auf all deinen Geräten • Warnungen bei schwachen oder kompromittierten Zugangsdaten erhalten	Alles von Individual, plus: • Lade bis zu 5 Familienmitglieder ein • Unbegrenzte Tresore teilen • Verwalte den Zugriff mit einfachen Admin-Kontrollen	• Teile Passwörter und sensible Daten • Bleib auf dem Laufenden mit umsetzbaren Sicherheitswarnungen. • Zugriff mit rollenbasierten Berechtigungen zuweisen • Entwickle sicher mit 1Password Entwickler-Tools • Erhalte Hilfe mit freundlichem Support und Onboarding-Ressourcen.	Enthält das Starterpaket für Teams und außerdem: • Integration mit Okta, Entra ID, OneLogin, Duo und mehr • Arbeite sicher mit anderen zusammen mit rollenbasierter Tresorfreigabe und Berechtigungen. • Stärke Sicherheitspraktiken mit Watchtower-Warnungen.

Individual

Perfekt für eine einzelne Person, um alle privaten Passwörter und Daten zu sichern.

Families

Bietet die gleichen Funktionen wie der Individual-Plan, aber für bis zu 5 Familienmitglieder. Jeder bekommt seinen privaten Tresor, zusätzlich können

gemeinsame Tresore für die Familie erstellt werden.

Starterpaket für Teams

Ideal für kleine Teams (bis zu 10 Personen). Der Fokus liegt auf der sicheren Zusammenarbeit: Passwörter und Dokumente im Team teilen, Zugriffsrechte verwalten und Sicherheitswarnungen erhalten.

Business

Die umfassendste Lösung für Unternehmen. Enthält alle Funktionen des Team-Pakets und erweitert diese um erweiterte Sicherheitsfunktionen wie die Integration in bestehende Systeme (Okta, Entra ID), detaillierte Nutzungsberichte und individuelle Zugriffsregeln.

❓ **Hilfe! Master-Passwort vergessen?**

Das Master-Passwort ist der Schlüssel zu Ihrem Tresor. Falls Sie es vergessen haben, gehen Sie wie folgt vor:

1. **Biometrische Entsperrung nutzen:** Wenn Sie 1Password auf einem Gerät noch per Fingerabdruck oder Gesicht entsperren können, nutzen Sie diese Chance! Entsperren Sie 1Password und ändern Sie sofort Ihr Master-Passwort in den Einstellungen.
2. **Team-Administrator benachrichtigen:** Wenden Sie sich an Ihren Team-Admin oder IT-Verantwortlichen. Ein berechtigter Admin kann eine Account-Wiederherstellung für Sie durchführen.
3. **Kein Zugriff mehr möglich:** Falls keine der obigen Möglichkeiten greift, ist der Zugriff auf Ihren Tresor leider verloren. Aus Sicherheitsgründen kann 1Password Ihr Passwort nicht zurücksetzen oder umgehen.

Deshalb ist das Notfall-Kit und das sichere Merken des Master-Passworts so extrem wichtig!



Bei Fragen und Unklarheiten kontaktieren Sie mich gerne und jederzeit unter meiner
E-Mail Adresse: **cvzg@malerinstitut.de**