TERZO DIETIKON

Dig[iT]reff

# Password Manager

Donnerstag 28. Nov. 2024
10:00-12:00 Gleis21, Dietikon

Peter Kunz
pekudi@gmail.com

# Heutiges Programm

1. **Passwörter und Passkeys**
   Passwörter: Empfehlungen, Gefahren/Risiken, Passkeys und 2FA
2. **Passwortmanager**
   Definition, Funktionen, Arten
3. **Bitwarden und 1Password**
   Vergleich

## 15' Pause

4. **1Password**
   Erklärung, Installation, Vorgehen Schritt um Schritt

5. **ev. Tipps**

# Passwörter, Passkeys, 2FA

## Passwörter

1. **Funktion**: die geheime Zeichenfolge sichert die Identität eines Nutzers und verhindert unbefugten Zugriff.
2. **Starke Passwörter** bestehen aus mind. 12 Zeichen. Gross/Klein, Zahlen und Sonderzeichen ( ! @ # $ %^ ). Keine Muster, persönliche Daten oder reale Wörter.
3. **Einzigartiges Passwort** für jedes Konto.
4. **Passwortmanager** generieren sichere Passwörter, speichern sie und helfen diese zu verwalten.
5. **2-Faktor-Authentisierung** verwenden, wenn möglich

**Passwortliste**: notiere die Passwörter offline oder auf Papier, verwahre diese sicher und orientiere deine Vertrauensperson.

**Passwortgenerator und Passworttester**
=> https://www.roboform.com/de/password-generator
=> https://www.roboform.com/de/how-secure-is-my-password

# Passwörter, Passkeys, 2FA

## Passkeys

Passkeys ist eine sicherere Methode zur Authentifizierung, basierend auf kryptografischen Schlüsselpaaren.

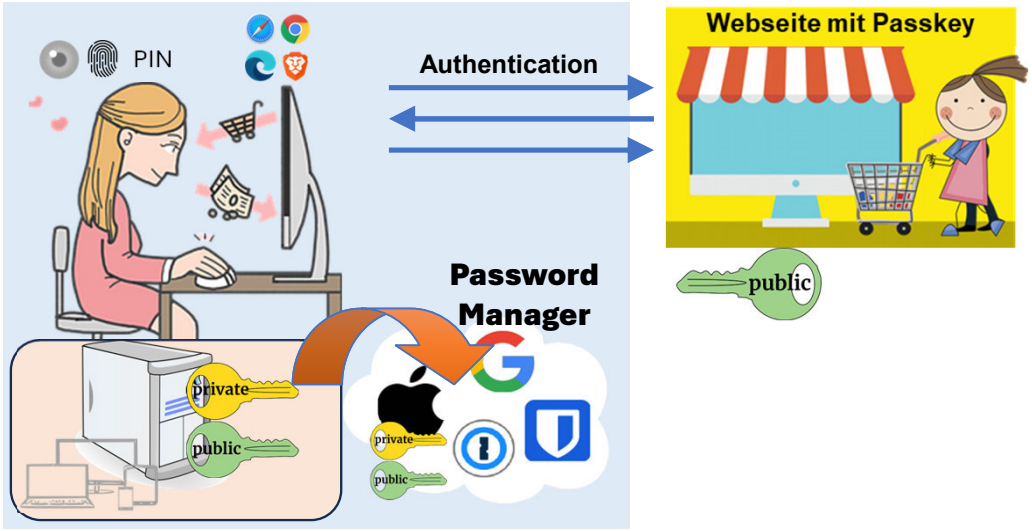
Ein Passkey besteht aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel bleibt auf dem Gerät oder dem Passwortmanager des Nutzers.
Der öffentliche Schlüssel wird mit dem Dienst (Webseite) geteilt.

Sie haben mehrere Vorteile:

1. **Sicherheit**: Passkeys eliminieren das Risiko von Passwort-Phishing, da der Nutzer nie ein Passwort eingeben muss.
2. **Benutzerfreundlichkeit**: Passkeys können einfach durch biometrische Daten (wie Fingerabdruck oder Gesichtserkennung) oder PINs verwendet werden.
3. **Kompatibilität**: moderne Geräte und Browser unterstützen Passkeys, was sie zu einer vielseitigen Lösung macht.
4. **Zukunft**: Passkeys werden Passwörter in vielen Bereichen ersetzen und so die Sicherheit und Benutzerfreundlichkeit verbessern.

## Passwörter und Passkeys im Passwortmanager

Moderne Passwormanager unterstützen das Generieren und Verwalten von Passkeys. Der Passkey ist dann nicht mehr an ein Gerät gebunden.




siehe auch Dig[iT]reff Präsentation "Passkeys"
https://terzo-dietikon.ch/wp-content/uploads/DigiTreff-20240821-PassKeys.pdf

# Passwörter, Passkeys, 2FA

**2FA, Zwei-Faktor-Authentisierung** ist ein Sicherheitsverfahren, bei dem zwei verschiedene Faktoren verwendet werden, um eine Identität zu bestätigen.

**1. Faktor: etwas, das du weisst**: typischerweise Benutzername/E-Mail und Passwort oder eine PIN.

**2. Faktor: etwas, das du hast**: meist ein Smartphone, ein SMS-Code, eine Authentifizierungs-App oder ein Token-Gerät.

- **Erhöhte Sicherheit**: wenn Passwort gestohlen wird, kann Angreifer ohne den 2. Faktor nicht auf Konto zugreifen.
- **Schutz vor Phishing**: auch bei Phishing, kann der Angreifer nicht ohne den 2. Faktor auf dein Konto zugreifen.

**Beispiel für 2FA**:
Anmelden mit Passwort (1. Faktor) und dann bestätigen mit Code, der auf das Smartphone (2. Faktor) gesendet wurde.

**2FA Methoden**:

- SMS-Codes: ein Code wird per SMS an das Smartphone gesendet.
- Authenticator: Apps von Google, Apple, Microsoft generieren zeitbasierte Einmalpasswörter (TOTP).
- Biometrische Daten: Fingerabdruck-, Gesichts- oder Iriserkennung.

**Es lohnt sich, 2FA für alle wichtigen Konten anzuwenden, um die eigene Sicherheit erheblich zu erhöhen.**

# Passwortmanager – was ist das?

**Ein Passwortmanager ist eine Software,
die Passwörter in einem digitalen Tresor sicher speichert.**


- Sichere, stark verschlüsselte Speicherung von Passwörtern, Passkeys, Kreditkarteninformationen und anderen Daten. Einfache Organisation mit Kategorien und Tags.
- Erhöhte Sicherheit durch Vergabe von starken, einzigartigen Passwörtern oder Phrasen.
- Automatische Eingabe von Anmeldedaten auf Websites und in Apps. Zugriff von verschiedenen Geräten und Plattformen aus.
- Zwei-Faktor-Authentizierung, 2FA für zusätzliche Sicherheit.
- Überwachung der Konti und Anmeldedaten: Hinweis auf geleakte Plattformen, schwache oder mehrfach gebrauchte Passwörter, Einsatz von 2FA oder Passkeys.

# Passwortmanager – wozu?

Passwortmanager verbessern die Sicherheit und den Komfort bei der Verwaltung von Passwörtern und anderen sensiblen Daten. Sie sind ein unverzichtbares Werkzeug für jeden, der seine Online-Sicherheit erhöhen möchte.

1. **Sicherheit**: Erstellt und speichert starke, einzigartige Passwörter.
2. **Bequemlichkeit**: Sie müssen sich nur ein Master-Passwort merken.
3. **Synchronisation**: Zugriff auf Passwörter über verschiedene Geräte hinweg.
4. **Teilen**: Sicheres Teilen von Passwörtern mit anderen.
5. **Überwachung**: Warnt vor schwachen oder gefährdeten Passwörtern.
6. **Zero-Knowledge**: Daten werden verschlüsselt gespeichert und übertragen.
7. **Zusätzlich**: gute Passwortmanager nehmen auch Kreditkarten- und andere wichtige Informationen auf.
   ⇨ ersetzt ev. die Zugangsliste für den Digitalen Nachlass (Dig[iT]reff vom 25.4.2024 )

Als Nachteile sind zu erwähnen: gewisser Aufwand auf Passwortmanager zu wechseln, Gefahr des Verlustes des Masterpasswortes, SPoF d.h. ein zentraler Angriffspunkt, ev.  kein Zero Knowledge Management, ev. nicht Plattform übergreifend

# Passwortmanager – verschieden Arten

Es gibt verschiedene Arten von Passwortmanagern, die jeweils unterschiedliche Funktionen und Sicherheitsmerkmale bieten.

- **Betriebssystem-integrierte Passwortmanager**: Apple und Microsoft bieten eigene Passwortmanager an.
  z.B: **Passwörter** von Apple oder **Authenticator** und **Hello** von Microsoft
- **Browserbasierte Passwortmanager**: sind integriert in Webbrowser, wie z.B. **Chrome**, **Firefox** oder **Brave**.
  Sie speichern Passwörter und bieten Autofill-Funktionalität.
- **Cloudbasierte Passwortmanager** speichern Passwörter in der Cloud, so kann von verschiedenen Geräten und Plattformen zugegriffen werden. Beispiele sind **Bitwarden** und **1Password**.
  Beide sind preiswert: kostenlos bis ca. 10.- bis 30.-/Jahr und noch günstigere Familienpakete.
  Sie speichern auch Karten-, ID- und andere Informationen;
  Zusatzdienste wie PW-Analysen, PW teilen, sicheres Senden, Dateispeicherung, Leak-Erkennung ...
  Beide unterstützen Browsererweiterungen.
- **Lokale Passwortmanager**: speichern Passwörter auf dem lokalen Gerät und bieten daher eine höhere Sicherheit. Beispiele sind **KeePass** und Enpass

# Apples neue iOS "Passwörter" App

**"Darum nutze ich Apples neue Passwörter App NICHT (iOS 18)"**

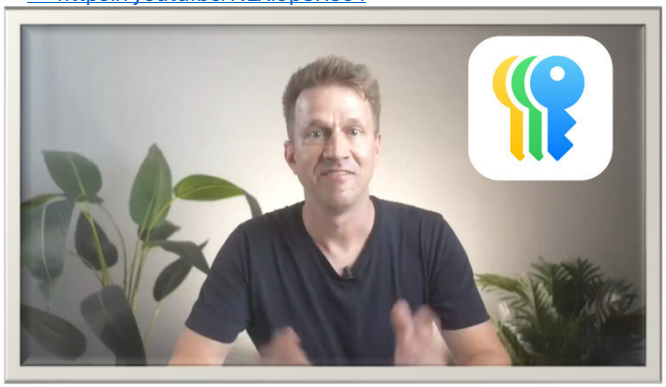
**Zusammenfassung des Videos vom August 2024**

Welcher Passworttyp bist du? app ab iOS 18 ab Sep. 2024, Funktionen, Vor-/Nachteile, Hinweis auf Passkeys, 2FA, schlechte Passwörter.

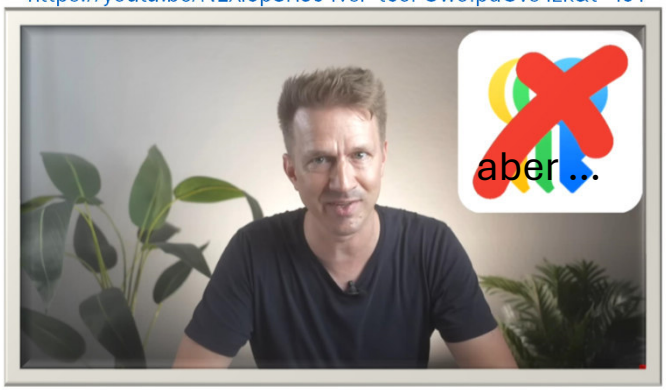
Ist gut und benutzerfreundlich aber:

- **Zugang nur mit iPhone Entsperrcode geschützt → NoGo!**
  **Wer diesen kennt, hat Zugriff auf Benutzername, Passwörter, Anmeldeseiten, 2FA Codes und E-Banking**
- limitierte Funktionen: nur Passwörter, keine Gruppierung oder Tags, Sicherheitsberichte, PW-Generator
- nur für reine Apple Welt tauglich, nicht Quellcode offen
- Verlust des Zugangs heisst Verlust aller Passwörter

**Teil 1** **5:48 Min**
=> https://youtu.be/NLXi9pSR364



**Teil 2** **4:52 Min**
https://youtu.be/NLXi9pSR364?si=t6cFGwoIpdGvs4zk&t=491



# Browserbasierte Passwortmanager

Alle gängigen Browser (Edge, Chrome, Safari, Brave …) haben heute einen eigenen Passwortmanager integriert, dieser ist meist standardmässig bereits aktiviert.

**Es ist besser den eingebauten Passwortmanager zu verwenden als gar keinen!**

Es ist eine praktische Möglichkeit, besser mit Passwörtern umzugehen.

Die browserbasierten Passwortmanager sind benutzerfreundlich aber reichen nicht an die Sicherheitsfunktionen und -merkmale der Drittanbieter-Optionen heran.

Funktionen sind beschränkt.

**Ein Wechsel auf auf eigenständige Passwortmanager empfiehlt sich.**

Die Daten dieser Passwortmanager können gut als CSV-Datei exportiert und in eigenständigen Passwortmanager importiert oder sogar direkt eingelesen werden.

# Bitwarden vs 1Password

=> https://www.youtube.com/watch?v=SkWSHTnAisY 14:36

Gutes, informatives Video von Cybernews vom Juli 2024


**"Bitwarden vs 1Password | Wer ist besser im Jahr 2024?**

*"Beide bieten exzellente Funktionen und Sicherheitsstandards,*

- *aber welcher ist für dich am besten geeignet?*
- *Heute werden wir beide Passwortmanager genauer unter die Lupe nehmen und am Ende dieses Vergleichs sollten bestenfalls keine Fragen mehr offen sein."*

VIDEOKAPITEL



## Zusammenfassung des Videos

Sicherheit, Zero-Knowledge-Architektur, 2FA, externe Audits, Secret Key, Funktionen, Passkeys, Import, PW-Generator, PW-Sharing, Autofill, Send, Berichte/Watchtower, Reisemodus, Kosten, Rabat, Kompatibilität, Benutzerfreundlichkeit, Support

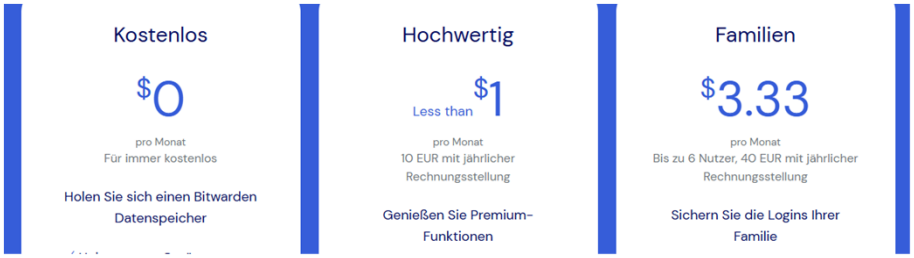
# Bitwarden vs 1Password - Abos

Möchte man einen unabhängigen Passwortmanager, so empfehle ich
**Bitwarden oder 1Password, die sich beide gut für verschiedene IT-Plattformen eignen.**

Interessant ist das kostenlose Abo von Bitwarden für Einzeluser oder die Abos für Familien

**Bitwarden** => Bitwarden.com/de-de

Als Open-Source sicher und zuverlässig
Benutzerfreundliche Oberfläche
Fr. 0.- bis 40.- für Familien pro Jahr




**1Password** => 1password.com/de

Benutzerfreundlicher, responsiv und kompatibel
Mehr Funktionen
Fr. 36.- bis 60.- für Familien pro Jahr

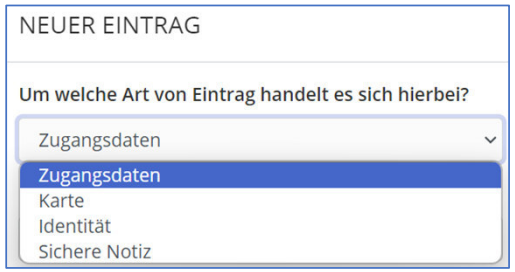
# Bitwarden vs 1Password – Einträge und Berichte

Der Funktionsumfang beider Passwortmanager ist ähnlich.

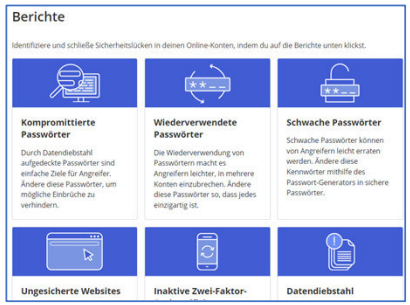
1Password hat mehr Kategorien verfügbar und ist moderner in der Darstellung.

**Bitwarden** => Bitwarden.com/de-de

neuer Eintrag

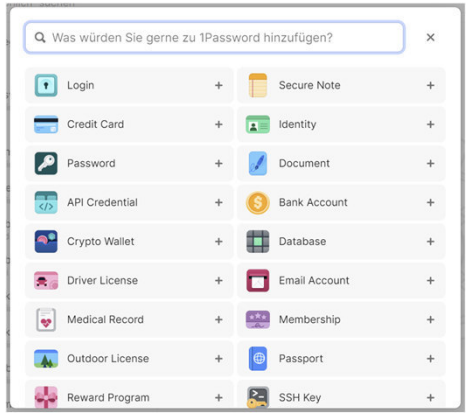



Berichte




1Password => 1password.com/de

neuer Eintrag




Watchtower

# 1Password Tutorial 13.8.2024

=> https://www.youtube.com/watch?v=gpu7CulgPXA 8:37 Min

## Video von Fabi - Ausführliche Anfänger-Anleitung!

*"1Password bringt dich der absoluten Passwortsicherheit einen Schritt näher ..."*

## Zusammenfassung des Videos

Abo, Installation, Masterpasswort, Funktionen, Presets für Einträge, Autofill, PW-Generator, Sicherheit, Audits, Tresore und Freigabe, Reisemodus, PW-Sharing, Watchtower, Passkeys,

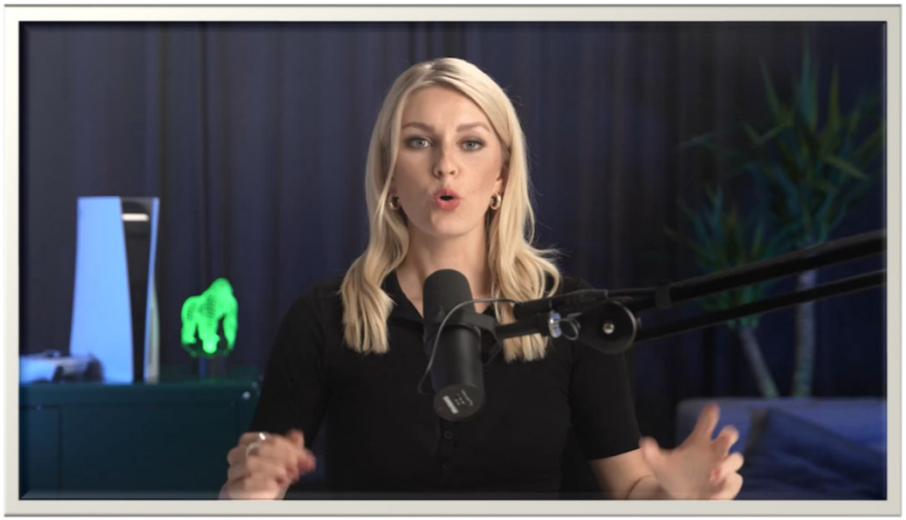

VIDEOKAPITEL
00:43 1Password herunterladen und installieren!
01:31 1Password Täglicher Gebrauch!
03:16 1Passwörter Tresore!
04:04 Reisemodus!
04:29 Objekte freigeben!
05:04 Watchtower!
05:29 Passkeys!
06:24 Automatisch gelöschte Zwischenablage!
06:46 1Password Preise!
07:12 1Password für Familien?
08:15 Fazit - Wie nutzt man 1Password?

# 1Password Anleitung 18.11.2024

=> https://www.youtube.com/watch?v=rHx94J5dZoI 8:49 Min

## Video - Wie man 1Password Funktionen verwendet!

*"In dieser Anleitung zeige ich dir, wie du 1Password sowohl für Anfänger als auch für Fortgeschrittene verwenden kannst."*



## Zusammenfassung des Videos

Installation, Login, PW erfassen, Kategorien, Tresore, Teilen, Sicherheit, Secret Key pro Gerät, Import von Browser Passwörtern, Familientarif, Watchtower, PW-Generator, Passkeys, Browser Erweiterungen, Support, Preise

VIDEOKAPITEL
00:39 1Password-Tutorial - Anleitung für Anfänger
04:57 Wie man 1Password wie ein Profi benutzt
06:38 Ist 1Password mit allen Geräten kompatibel?
07:36 Ist 1Password es wert?
08:17 Fazit – solltest du 1Password verwenden?

# 1Password Family Tutorial Ausgabe 1.2.2024

=> https://youtu.be/pL-fE9seQ_4?si=oAe9AwZGQDL9Qkyg 9:58 Min

## Video von Fabi - Lerne alles, was du wissen musst!

*"... Dieser 1Password-Tutorial für Familien zeigt eine effiziente Lösung, um die ganze Familie zu schützen ..."*

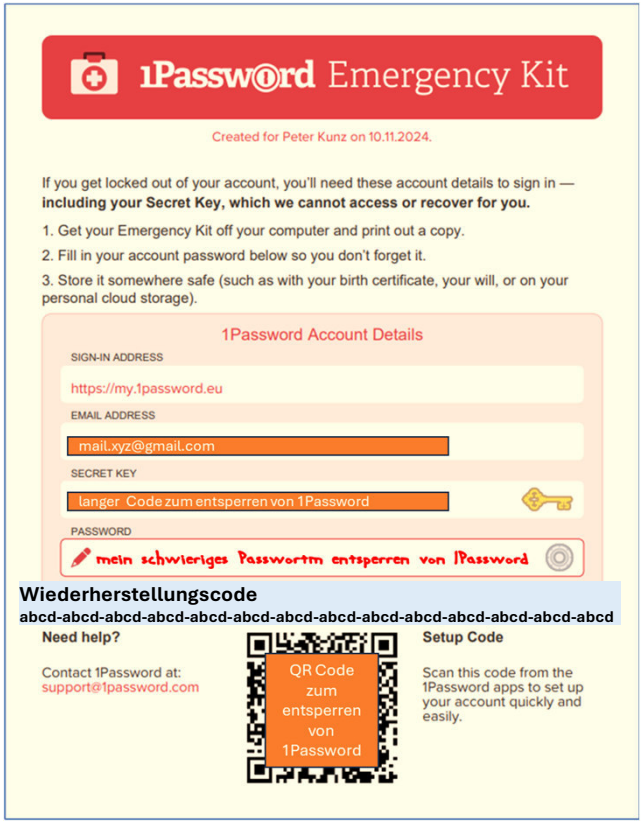

## Zusammenfassung des Videos

Einstieg in 1Password und Einrichtung werden sehr gut erklärt.

Abo, Installation, Passwörter verwalten, teilen und generieren, Browsererweiterungen, Watchtower, Reisemodus, Secret Key, Zero-Knowledge Technologie

VIDEOKAPITEL
0:25 1Password Family Preise und Tarife
1:08 1Password Family Tutorial
2:35 1Password Passwörter verwalten und freigeben
3:35 1Password Passwörter generieren!
4:04 1Password Tresore
4:31 Wie benutzt man 1Password Tresore?
6:12 1Password Browser-Erweiterung
6:49 1Password Sicherheit und zusätzliche Funktionen
8:47 Fazit

# 1Password – Emergency Kit  und Wiederherstellungscode


1Password Emergency Kit

Created for Peter Kunz on 10.11.2024.

If you get locked out of your account, you'll need these account details to sign in — **including your Secret Key, which we cannot access or recover for you.**

1. Get your Emergency Kit off your computer and print out a copy.
2. Fill in your account password below so you don't forget it.
3. Store it somewhere safe (such as with your birth certificate, your will, or on your personal cloud storage).

1Password Account Details

SIGN-IN ADDRESS
https://my.1password.eu

EMAIL ADDRESS
mail.xyz@gmail.com

SECRET KEY
langer Code zum entsperren von 1Password

PASSWORD
mein schwieriges Passwortm entsperren von 1Password

**Wiederherstellungscode**
abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd-abcd

**Need help?**
Contact 1Password at:
support@1password.com

QR Code zum entsperren von 1Password

**Setup Code**
Scan this code from the 1Password apps to set up your account quickly and easily.

Das Emergency Kit PDF gilt pro Person, enthält Anmeldedaten, Secret Key und ein Platz, um das Masterpasswort zu notieren.

Es dient dazu, wieder Zugriff auf das 1Password-Konto zu erhalten.

Während der Installation wird das Emergency Kit erzeugt. Drucke ihn aus. Ergänze diesen mit dem **Passwort** und **Wiederherstellungscode** .

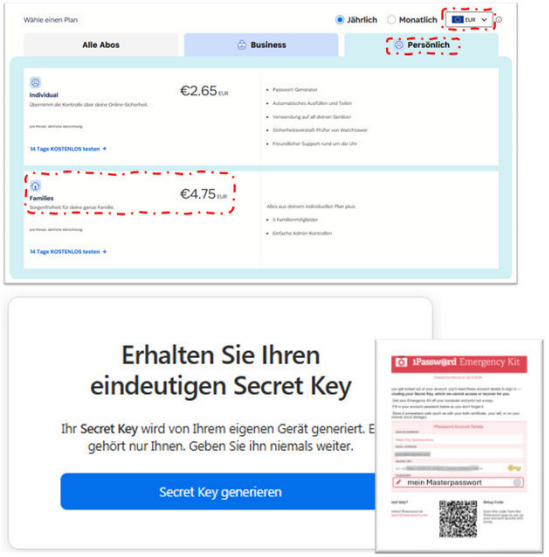
**Bewahre das Emergency Kit sicher auf!!**

Du kannst das Kit im nachhinein ausdrucken:
- Login  https://my.1password.eu
- klick auf dein Name rechts => wähle 'Mein Profil'
- wähle 'Emergency Kit speichern'

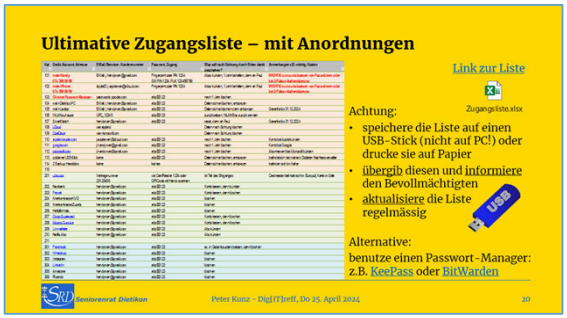
Dort findet sich auch der **Wiederherstellungscode** für dein Gerät, mit welchem wieder auf 1Password zugegriffen werden kann, falls Passwort und Geheimschlüssel verloren gingen.

# 1Password – Schritt um Schritt

1. **Sichern** existierende Passwörter, bereitstellen/exportieren/bereinigen
2. **Lernen** => [1Password Tutorial 2024 | Ausführliche Anfänger-Anleitung]!
3. **Installation** 1Password => [1password.com/de] (bzw. [Bitwarden.com/de-de])
   Einrichten auf Desktop und Smartphone. Browsererweiterung aktivieren
   **!!! Emergency Kit und Wiederherstellungscode drucken !!!**
   Empfehlung: 2. Konto einladen mit Vollzugriff als Backup
4. **Importieren** oder erfassen der Passwörter bzw. Zugangsinformationen
   Empfehlung: paketweiser (5-10) Import nach Priorität
   Sofort bei allen ein neues, starkes PW erstellen
5. **Bereinigen** der Passwörter, Watchtower aufrufen und Hinweise beachten
6. **Teilen** der Passwörter mit Tresoren, ev. Reisetresor erstellen
7. **Exportieren** und Ausdrucken der Passwörter und sicher versorgen



# 1Password als ultimative Zugangsliste im digitalen Nachlass




1Password

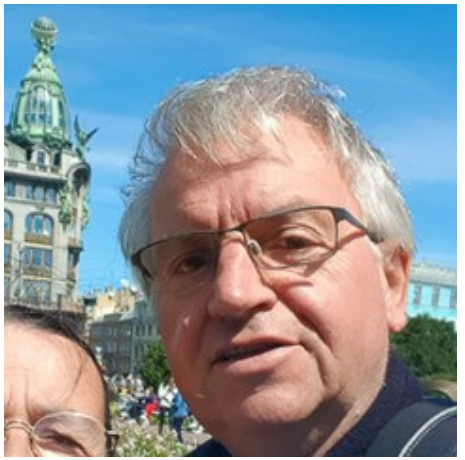

**Im Dig[iT]reff April 2024 => Digitaler Nachlass wurde die 'Ultimative Zugangsliste' vorgestellt, in welcher alle wichtigen Zugänge, Passwörter und zugehörigen Anordnungen gespeichert werden.**

Diese Liste kann nun inkl. der Anordnungen schrittweise in 1Password übernommen und somit ersetzt werden.

In der Anordnung für den Todesfall muss das dann vermerkt und auch die Vertrauensperson muss orientiert werden.

☒ Digitaler Nachlass (Computer, Smartphone, Tablets, E-Mail, Facebook, Benutzerkonten/Daten im Internet usw.)
Ich habe eine Liste mit den Zugangsdaten (Benutzernamen/Passwörter) erstellt.
☒ Physisch – Das Dokument befindet sich: Emergency Kit, im Safe bei Vorsorgeauftrag/Testament
☐ Auf meinem PC – Dateiname/Passwort: _____
☒ Auf einem USB Stick – Aufbewahrungsort/Passwort: bei meinem Bevollmächtigten, Sohn Paul
☐ In einem Online-Speicher: ☐ Swisscom Docsafe ☐ SecureSafe ☒ Anderer:
Zugangsdaten: in 1Password - "mein 3$+ schwierigesPassword"

# Peter Kunz, 1954



- 2018 – 2023 Webmaster des Seniorenrat Dietikon
- Mitglied ehemalige Computeria, Initiant des Dig[iT]reffs
- Ausbildung: Dipl. Ing. Agr ETH / eidg. dipl. Organisator / Web Publisher SIZ u.a.
- über 30 Jahre in Informatik tätig: Organisation, Management, Business Process Reegineering, Benutzerschulung, Projektmanagement
- seit 40 Jahren im Limmattal, davon 38 in Dietikon, verheiratet mit Vreni, 4 Söhne
- Hobbies: Informatik, Hund, Reisen, Velotouren, Lesen, Werken

✉ pekudi@gmail.com ✆ 076 746 74 80