



Security etc. (Passwortmanager oder Zettel?)

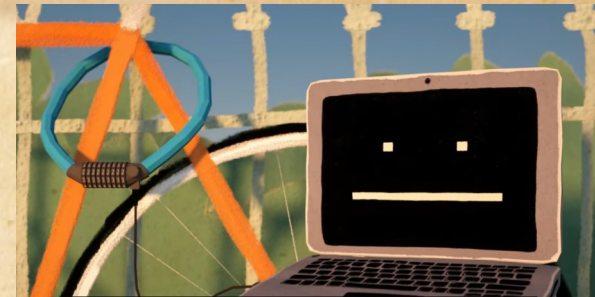
- Passworte ausdenken und verwalten
 - Passkey: Vergleich mit Passwort
 - Passwortmanager zum Verwalten
- 

Passworte ausdenken und verwalten

Was ist eigentlich ein Passwort?

Wie kann ich das „Knacken“ erschweren?

<https://www.youtube.com/watch?v=jtFc6B5lmIM>



Muss ich für jede Anwendung ein eigenes Passwort verwenden und sollte ich es jeden Monat wechseln?

Jörg Schieb rät: wie erzeuge ich sichere Passworte und wie verwalte ich sie?

Passwort-Manager ja/nein

Müssen Passwortmanager auf allen Endgeräten, die ich nutze, installiert sein?

Was ist mit den Geräten, die ich an meinem Arbeitsplatz oder im Internet-Café oder im Hotel nutze?

<https://www.youtube.com/watch?v=jfsJ1b-RAWs>

<https://checkdeinpasswort.de/>

Passkey

Was ist ein Passkey?

Passkeys basieren auf einem ausgeklügelten System der asymmetrischen Verschlüsselung:

Das Schlüsselpaar: Sobald Sie einen Passkey für eine Website oder App erstellen, generiert Ihr Gerät zwei zusammengehörige Schlüssel.

Der öffentliche Schlüssel (**Public Key**): Dieser wird beim jeweiligen Anbieter (z.B. Google, Amazon, PayPal) hinterlegt.

Der private Schlüssel (**Private Key**): Dieser verbleibt sicher und verschlüsselt auf Ihrem Gerät (z. B. im Secure Element Ihres iPhones oder Android-Smartphones).

Die **Authentifizierung**: Der Anbieter-Server sendet beim Login eine mathematische Anfrage an Ihr Gerät. Ihr Gerät verifiziert Sie als rechtmäßigen Besitzer (z. B. via Face ID, Touch ID oder PIN) und beantwortet die Anfrage. Der private Schlüssel verlässt dabei zu keiner Zeit Ihr Gerät.

Leider bieten noch nicht alle Anbieter das Passkey-Verfahren an!

Passkey

Wie funktioniert der Passkey?

Sie melden sich an (z. B. bei Google oder Ihrer Bank).

Ihr **Handy, Tablet oder Computer** fragt:

„Möchten Sie sich anmelden?“ → Sie tippen auf **"Ja"**.

Oder: „Geben Sie Ihre PIN ein“

Oder: „Berühren Sie den *Fingerabdruck-Sensor*“ oder FaceId
(wenn Ihr Gerät das kann).

Fertig! Sie sind drin – **ohne Passwort**.

Vorteile:

- ✓ **Kein Merken nötig** – der Schlüssel ist **sicher in Ihrem Gerät gespeichert**.
- ✓ **Sicherer** – Betrüger können ihn **nicht stehlen** (weil er nur auf **Ihrem Gerät** funktioniert).
- ✓ **Schneller** – kein Tippen mehr, nur **ein Klick oder Fingerabdruck**.
- ✓ **Einfach** – wie das Aufschließen Ihrer Haustür mit dem **eigenen Schlüsselbund**.

Passwort versus Passkey

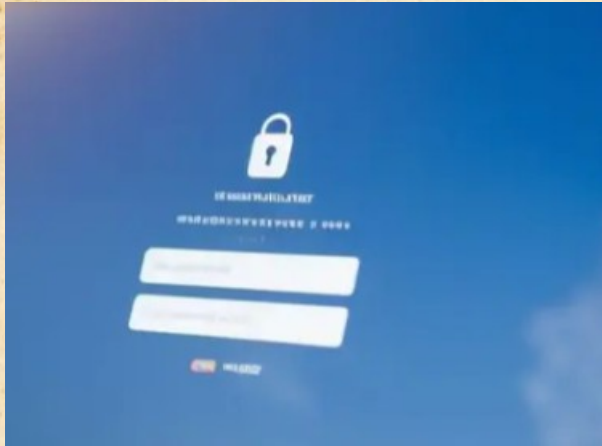
Vergleich: Wie ein Schloss zu Hause

Passwort	Passkey
Sie brauchen einen Schlüssel (Passwort), den Sie überall mitnehmen müssen.	Ihr Handy oder Laptop ist der Schlüssel – Sie brauchen nur Ihre PIN oder Fingerabdruck .
Wenn jemand den Schlüssel klaut , kann er Ihr Haus öffnen.	Der Schlüssel funktioniert nur bei Ihnen – selbst wenn jemand Ihr Handy stiehlt, kann er ihn nicht nutzen .
Sie müssen viele Schlüssel (Passwörter) für verschiedene Türen (Websites) haben.	Ein Schlüssel (Passkey) pro Tür – Ihr Gerät erledigt den Rest.

Fragen

- ◆ "Muss ich mir den Passkey merken?" → Nein! Der Passkey ist wie ein unsichtbarer Schlüssel in Ihrem Handy oder Computer. Sie brauchen nur Ihre **PIN oder Fingerabdruck**.
- ◆ "Was, wenn ich mein Handy verliere?" → Keine Sorge! Sie können **Backups** machen (z. B. in der iCloud oder bei Google). Dann bekommen Sie Ihre Passkeys auf einem **neuen Gerät** zurück.
- ◆ "Funktioniert das überall?" → Noch nicht. Aber **immer mehr Seiten** (wie Google, Microsoft, PayPal) unterstützen Passkeys. Für andere Seiten nutzen Sie weiter **Passwörter + einen Passwort-Manager** (z. B. Bitwarden).
- ◆ "Ist das wirklich sicher?" → Ja! Passkeys sind **viel sicherer** als Passwörter, weil Betrüger sie **nicht stehlen oder erraten** können.

Passwortmanager Überblick



Ein Passwort-Manager speichert alle Passwörter verschlüsselt an einem sicheren Ort.

Nutzer brauchen nur noch ein Master-Passwort.

Mit einem Passwort-Manager können Sie starke Passwörter automatisch erstellen lassen.

Lokale oder Cloud-Speicherung: Beide Varianten bieten Vor- und Nachteile.

Alternativen zum Passwort-Manager sind Passkeys oder das Notieren von Passwörtern auf Papier oder in einer Textdatei.

Siehe auch:

<https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sind-passwortmanager-sinnvoll-114154>

Passwortmanager-Funktionen

Ein Passwort-Manager ist ein digitaler Tresor für Ihre Zugangsdaten. Er speichert Benutzernamen, Passwörter und andere Login-Informationen in der Regel verschlüsselt – geschützt durch ein einziges Master-Passwort.

Dieses **Master-Passwort** sollte besonders stark sein – und Sie dürfen es nicht vergessen. Ist das Master-Passwort verloren, besteht eventuell keine Möglichkeit mehr, Ihre Daten wiederherzustellen.

Automatisches Ausfüllen: Login-Daten werden auf Websites oder in Apps sicher eingefügt.

Passwort-Generator: Erstellt zufällige, starke Passwörter auf Knopfdruck. Sie müssen sich keine Gedanken über die Vergabe eines starken Passwortes machen.

Synchronisation: Auf Wunsch und sofern möglich Zugriff von mehreren Geräten über eine verschlüsselte Cloud-Verbindung.

Warnung vor möglichen Phishing-Angriffen und manipulierten Websites, zum Beispiel wenn sich die URL der aufgerufenen Webseite von der im Passwort-Manager gespeicherten unterscheidet.

Zwei-Faktor-Authentisierung (2FA): Zusätzliche Sicherheitsebene gegen unbefugten Zugriff.

Überall, wo Sie sich mit einem Passwort anmelden, gilt grundsätzlich: Sie sollten die Sicherheit bei Logins erhöhen, indem Sie die **Zwei-Faktor-Authentisierung (2FA)** aktivieren. Dabei geben Sie nicht nur ein Passwort ein, sondern bestätigen den Login mit einem weiteren Merkmal. Das kann ein Code sein, der Ihnen per E-Mail oder SMS geschickt wird, oder in einer entsprechenden App erscheint, der nur kurze Zeit gilt. Auch per Gesichtserkennung oder Fingerabdruck kann eine Authentisierung möglich sein.

Passwortmanager-Typen

Cloud-Passwortmanager:

Die Daten werden verschlüsselt auf den Servern des Anbieters gespeichert und automatisch über alle Ihre Geräte (PC, Smartphone) synchronisiert. Vorteil: Sehr bequem, ortsunabhängiger Zugriff.

Lokaler Passwortmanager:

Der Passwort-Tresor liegt ausschließlich lokal auf Ihrem eigenen Gerät (Festplatte, USB-Stick). Vorteile: Höchste Kontrolle, keine Daten in der Cloud.

Browser-integrierter Manager: Feste Bestandteile von Chrome, Firefox oder Edge.

Vorteile: Kostenlos, erfordern keine Installation. Nachteile: Eingeschränkter Funktionsumfang, geräteübergreifend oft umständlich.

Daneben gibt es noch **Hardware-basierte Manager:** Spezielle physische Geräte, die Logins speichern und teils Passwörter direkt über USB eingeben.

Oder **Self-Hosted-Manager:** Open-Source-Lösungen, die Sie auf Ihrem eigenen Heimserver betreiben.

Fragen zur Entscheidungsfindung:

Nutzen Sie den Passwortmanager allein oder im Team/der Familie?

Nutzen Sie ihn auf mehreren Geräten?

Ist Ihnen bequeme Synchronisation oder maximale Kontrolle wichtiger?

Kostenfreie Passwortmanager

1. Bitwarden (Top-Empfehlung)



Warum gut:

- Komplette kostenlos nutzbar (auch dauerhaft)
- Funktioniert mit **Apps & Browsern**
- Autofill auf Android & iOS (füllt App-Passwörter automatisch aus)
- Synchronisiert auf beliebig vielen Geräten
- Open Source (sehr transparent & sicher)

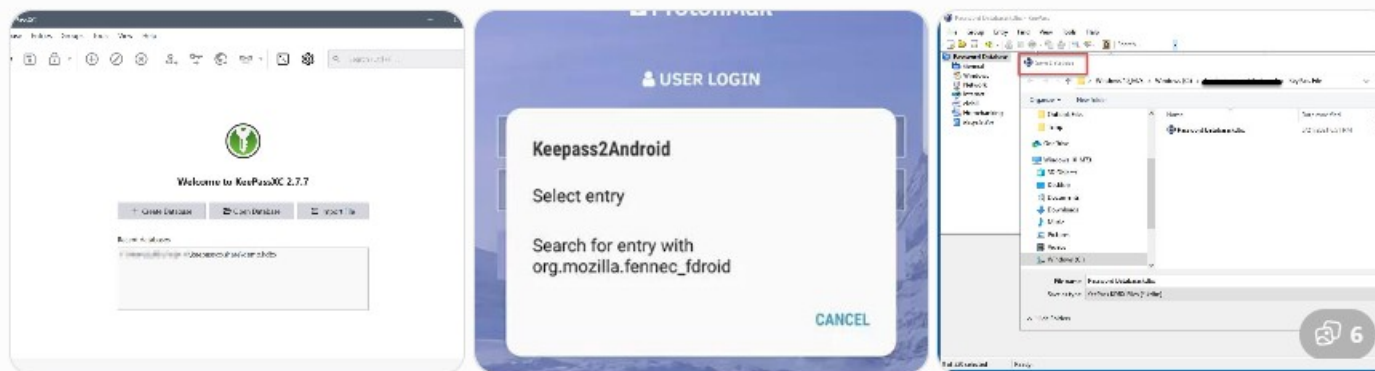
Einschränkung:

- Einige Extras (z. B. 2FA mit Hardware-Key) kosten ~10 €/Jahr (optional)

👉 **Fazit:** Beste kostenlose Lösung für die meisten Nutzer

Kostenfreie Passwortmanager

2. KeePass (+ Varianten wie KeePassXC / KeePass2Android)



Warum gut:

- 100 % kostenlos & Open Source
- Deine Daten bleiben lokal (keine Cloud nötig)
- Mit Apps wie **KeePass2Android** → auch Autofill in Apps möglich

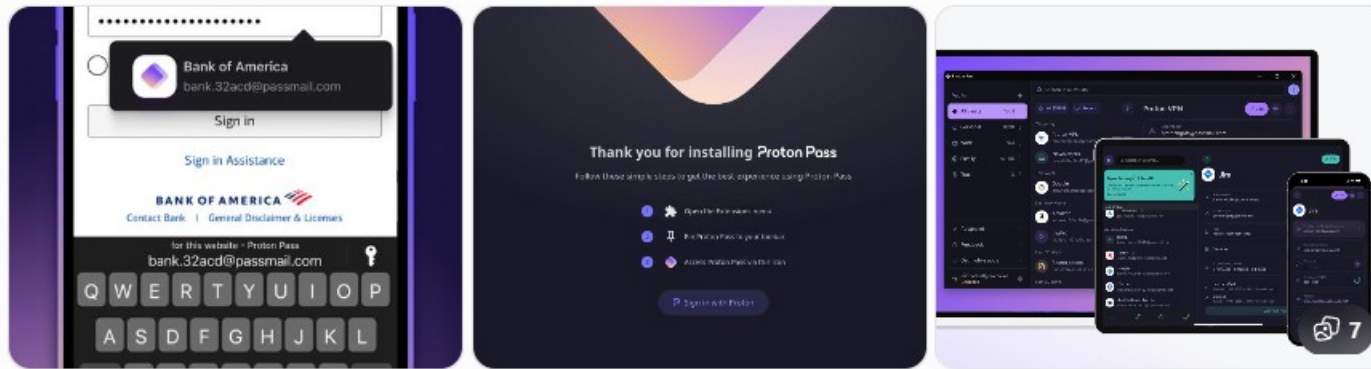
Einschränkung:

- Einrichtung etwas komplizierter
- Synchronisation musst du selbst lösen (z. B. über Dropbox)

👉 **Fazit:** Perfekt, wenn du maximale Kontrolle willst

Kostenfreie Passwortmanager

3. Proton Pass



Warum gut:

- Kostenloser Plan verfügbar
- Autofill in Apps (mobil)
- Starke Verschlüsselung (von Proton bekannt)

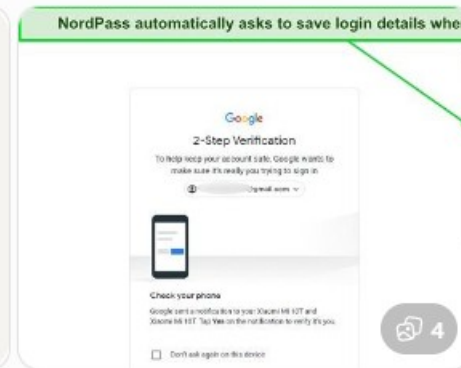
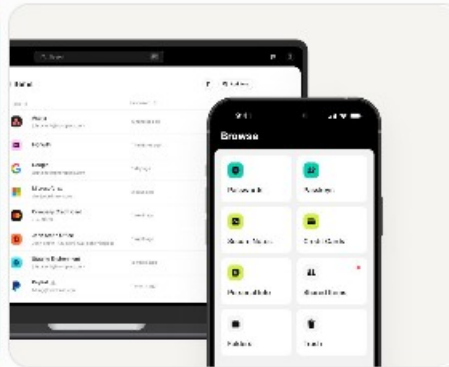
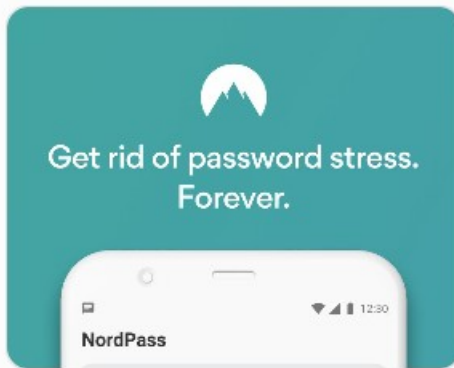
Einschränkung:

- Kostenlos etwas eingeschränkt (z. B. weniger Features als Premium)

 **Fazit:** Gute Alternative mit Fokus auf Datenschutz

Kostenfreie Passwortmanager

4. NordPass (eingeschränkt kostenlos)



Warum gut:

- Einfach zu bedienen
- Autofill auch in Apps

ABER:

- Kostenlos nur auf **einem Gerät gleichzeitig**
- Viele Funktionen nur Premium

 **Fazit:** Nur bedingt empfehlenswert gratis

Passwortmanager Fazit

Es gibt einige Passwortmanager, die nicht nur Browser-Logins sondern auch Apps (auf Smartphone und Tablet) unterstützen. Wichtig dabei ist „wirklich kostenfrei“, d.h. mit dauerhaftem Gratisplan ohne versteckte Gebühren.

Ein Passwort-Manager hilft Ihnen, den Überblick über Ihre Passwörter zu behalten. Sie können die Passwörter z.B. nach Anwendungen oder Personen strukturieren und auch Kreditkartennummern etc dort sicher speichern.

Nutzer brauchen nur noch ein Master-Passwort.

Mit einem Passwortmanager kann man starke Passwörter automatisch erstellen lassen.

Je nach Anforderung sollte man einen Passwortmanager wählen, der die Daten in der Cloud oder lokal speichert.

Damit ein Passwortmanager in einer App Passwörter ausfüllen kann, muss man bei
Android: “Autofill-Dienste“ aktivieren
Iphone: “Passwörter & Autofill“ aktivieren

Papier statt Passwortmanager

Vorteile einer Passwortsammlung auf Papier:

Die Passwörter können nicht durch schädliche Programme ausgelesen und gestohlen werden.

Wenn Sie eine Liste an einem sicheren Ort aufbewahren, können Erben oder von Ihnen bestimmte Bevollmächtigte etwa nach Ihrem Tod Ihre digitalen Konten schließen.

Nachteile einer Passwortsammlung auf Papier:

Insbesondere, wenn die Liste an einem leicht auffindbaren Ort aufbewahrt wird, wie beispielsweise in der Brieftasche oder unter der Tastatur, könnte sie schnell in falsche Hände geraten.

Aufwändig zu pflegen

Hat man die Liste nicht bei sich, kommt man unter Umständen nicht ins gewünschte Online-Konto.

Wo findet man die Vorträge vom Digital-Café?

Digital Mobil AWOthek

Zum Nachlesen der Vorträge

MVV neu in Landsberg

- [MVV-neu-in-Landsberg-02-2025](#)

ChatGPT

- [ChatGPT Übersicht 11-2025](#)
- [ChatGPT Anwendungsbeispiele 11-2025](#)

Elektronische Patientenakte (ePA)

- [ePA Infovortrag-05-2025](#)
- [ePA Status 01-2026](#)
- [ePA Beispiel TK-APP 01-2026](#)
- [ePA FAQ 05-2025](#)



Die neue **Digital Mobil AWOthek** enthält Vorträge und Dokumente zu den Themen unseres Digital-Cafés zum Nachlesen.

efi-landsberg.de/awothek

* Zu Problemen aller Art lesen Sie die Dokumentation und fragen Sie nach in der Digital-Mobil-Sprechstunde oder lesen Sie nach in der **AWOthek**!