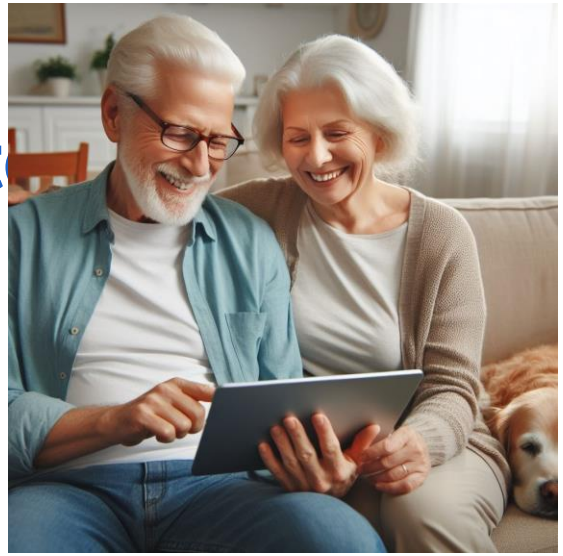
Dig[iT]reff

«Passkeys - das Ende der Passwört



Mittwoch, 21. August 2024, 10:00-12:00 im Gleis21, Dietikon

Referent: Peter Kunz

Heutiges Programm

- Kommunikation TERZO
- Passwörter
- Passkeys und Film

15′ Pause

- Beispiele Passkeys
- Passwortmanager

Passwörter – 3. Hauptprobleme

1. Unsichere Passwörter des Users

2. Schwachstellen (Leaks) beim Service

Meine Login Daten (E-Mail, Passwort etc.) können beim aufgerufenen Service gehackt und ev. entschlüsselt werden. Überprüfe dies:
- bei haveibeenpwned.com oder noch besser
- Beim Hasso Plattner Instituts sehpic..de/ilc/search

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
twitter.com (Dec 2021)	Dez. 2021	✓	208.868.809	–	Betroffen	–	–	–	–	–	–	–
	Dieser Leak enthält Identitätsdaten, die von der Domain twitter.com (Dec 2021) gescraped wurden.											
Leak Collection (Cit0day)	Nov. 2020		221.593.947	Betroffen	–	–	–	–	–	–	–	–
	Im November 2020 wurde eine Sammlung von mehr als 20.000 gehackten Websites unter der Bezeichnung "Cit0day" im Internet veröffentlicht. Die Sammlung umfasst mehr als 220 Millionen Zugangsdaten in Form von E-Mail-Adressen und Passwörtern, die häufig sowohl als Passwort-Hashes als auch im Klartext veröffentlicht wurden.											
123rf.com	Mär. 2020	✓	8.587.950	Betroffen	–	–	–	–	–	–	–	Betroffen
deezer.com	Sep. 2019	✓	228.657.974	–	–	Betroffen	–	–	–	–	–	–
	Dieser Leak enthält Identitätsdaten, die von der Domain deezer.com entwendet wurden.											
luminpdf.com	Apr. 2019	✓	15.454.875	–	Betroffen	–	–	–	–	–	–	–

3. Phishing

Der User **wird gedrängt** auf gefälschten Homepages seine Benutzerdaten einzugeben. Dies geschieht per E-Mail, SMS, Social Media, Brief mit QR-Code und telefonisch.

Phishing Beispiele

- **Dringendes Sicherheitsproblem!!** Per E-Mail oder auch Bildschirm PopUps wird dringlich gefordert, die Zugangsdaten zu bestätigen oder zu aktualisieren, um angebliche Sicherheitsprobleme zu lösen.
- **Sie haben gewonnen!!** Per E-Mail, WhatsUp und anderen sozialen Medien wird ein Preis, eine Erbschaft, ein super günstiger Kredit oder der passende Job angepriesen. Man soll nun persönliche Informationen eingeben, um diese zu erhalten.
- **Phishing-Websites** sehen aus wie die echten Seiten bekannter Unternehmen (z.B. Bank, Post, Swisscom). Sie fordern auf, sich einzuloggen, Kreditdateninformationen oder persönliche Daten zu aktualisieren, um diese Informationen zu stehlen.
- **SMS-Phishing (Smishing):** SMS von einem bekannten aber gefakeden Unternehmen fortert auf, einem Link zu folgen der Sie auf eine Phishing-Website führt, wo Sie aufgefordert werden, persönliche Daten einzugeben.
- **Telefon-Phishing (Vishing):** Betrüger geben sich als Mitarbeiter einer vertrauenswürdigen Firma (Microsoft, Bank etc.) aus und versuchen so auf sensible Informationen zu kommen und ev. führen sie auf eine Phishing-Website.

Wichtig!! **Wachsam sein und keine persönlichen Informationen preisgeben!**

Insbesondere, wenn:

- nicht sicher ist, ob die Anfrage legitim ist
- zeitlich und psychologisch Druck aufgesetzt wird etwas zu tun

Umfrage zu Passwörtern, Passkeys

Passwort-Fatigue ist real
Sieben von zehn Personen geben an, sich von der Anzahl der Passwörter, die sie sich merken müssen, überfordert zu fühlen. Wie sehen das die Dig[iT]reff-Teilnehmer?

- ☐ wer hält sich strikt an die Passwortregeln? / 50
- ☐ Wer denkt, dass seine Passwörter sicher sind? _____
- ☐ wer benutzt einen Passwortmanager? _____
- ☐ wer kennt Passkeys? _____
- ☐ wer benutzt Passkeys? _____

Adieu Passwörter - Willkommen Passkeys?

Das Thema «**Passkeys**» ist aktuell in aller Munde. Die Technologie wurde von der FIDO-Alliance entwickelt, der viele «Big Player» im Tech-Business angehören.

FIDO bedeutet «Fast Identity Online» (schnelle Online-Identifizierung).

- 2012 wurde der Grundstein für FIDO gelegt.
- 2018 wurde FIDO2 eingeführt. Die passwortlose Authentifizierung erfolgte mit einem **separaten USB Stick**.
- 2022 wurde eine Erweiterung des FIDO2-Standards, benannt als **Passkeys**, eingeführt.
  der FIDO2-Sicherheitsschlüssel kann nun auf dem **Smartphone/Tablet** oder PC liegen.
  Dadurch bieten immer mehr Online-Dienste die Möglichkeit an, sich mit Passkeys anzumelden.

Wenn von "Passkeys" die Rede ist, ist also passwortloses Anmelden gemeint.

Die Hoffnung vieler Fachleute ist, dass Passwörter durch Passkeys komplett abgelöst werden.

Probleme wie schwache Passwörter, das Stehlen von Userinformationen (Leaks) oder das Abgreifen sensibler Informationen durch Phishing könnten damit vorbei sein.

Das ENDE der PASSWÖRTER – willkommen PASSKEYS

Video von "The Morpheus Tutorials"
https://www.youtube.com/watch?v=CPUkHh6Y6BU
informatives und auch kritisches Video

13 Min

The Morpheus Tutorials
@TheMorpheusTutorials · 250.000 Abonnenten · 3045 Videos
Ein Kanal rund um das Thema Informatik und Programmieren mit über 2000 Videos! ...mehr
bio.link/themorpheus und 4 weitere Links

Podcast vom Bundesamt für Sicherheit in der IT
https://www.youtube.com/watch?v=m0J40Xczj14
sehr informativer Podcast mit einem Experten zum Hören

32 Min

Bundesamt
für Sicherheit in der
Informationstechnik

Firmen hinter der FIDO Alliance (Auswahl)

https://fidoalliance.org/members/

Big Player

Google, Apple, Meta, amazon, Microsoft

Passwortmanager

bitwarden, 1Password, LastPass, DASHLANE

weitere bedeutende Konzerne

intel, SAMSUNG, DELL, HUAWEI, NETFLIX, ebay, mozilla

Finanzkonzerne

PayPal, VISA, mastercard, HSBC, CB

Staatliche Organisationen

Federal Office for Information Security, Cabinet Office, NIST National Institute of Standards and Technology U.S. Department of Commerce

Wo werden Passkeys unterstützt?

Betriebssysteme

- **Apple Passkeys sind** integriert im iCloud Schlüsselbund der Geräte mit Touch ID oder Face ID https://www.passkeys.io/
- **Google Passkeys** sind mit Android Geräten kompatibel https://web.dev/articles/passkey-registration?hl=de
- **Microsoft Passkeys** integriert in Windows Hello https://developers.google.com/identity/passkeys?hl=de

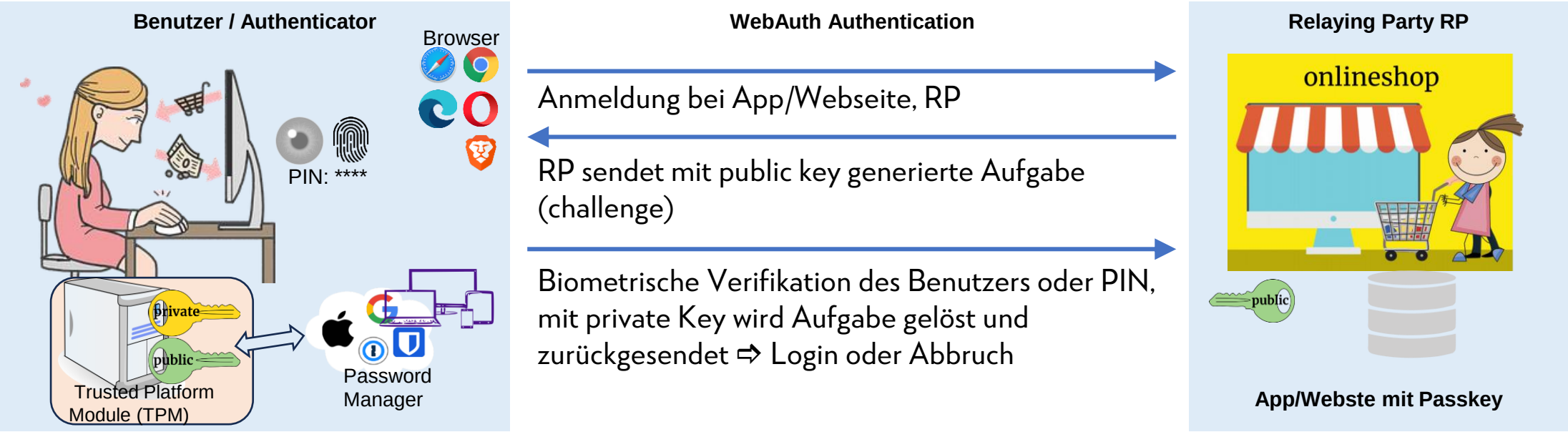
Browser	verfügbar auf Windows	macOS	Android	Linux
Google Chrome	✓	✓	✓	✓
Brave	✓	✓	✓	✓
Firefox	✓	✓	✓	✓
Microsoft Edge	✓	✓	✗	✗
Safari	✗	✓	✓	✗

Bei der Anmeldung über diese Browser bei einer Website die Passkeys unterstützt, kann einfach ein Fingerabdruck, die Gesichts-Authentifizierung oder ein PIN verwendet werden.
Dies ist eine nahtlose und sichere Möglichkeit sich anzumelden.

So funktionieren Passkeys (stark vereinfacht)

Passwortlose Authentifizierung mit Passkeys ist eine Methode zur Überprüfung der Identität eines Benutzers ohne die Eingabe eines Passworts.

Passkeys basieren auf asymmetrisch, kryptografisch erstellten Schlüsselpaaren (public and private Key).
Der öffentliche Schlüssel ist beim Onlineservice, der private Schlüssel auf dem Gerät des Benutzers gespeichert.



Vorteile der Passkeys gegenüber Passwörtern

Passkeys haben gegenüber Kennwörtern mehrere Vorteile,

- benutzerfreundlich und intuitiv.
- einfach zu erstellen und sie müssen weder gespeichert noch geschützt werden.
- für jede Website wird ein eindeutiges Schlüsselpaar (privater und öffentlicher) berechnet, dieses kann somit nicht wiederverwendet werden.
- äusserst sicher, da der private Schlüssel nur auf den Geräten des Benutzers gespeichert wird
- verhindern, dass Angreifer sie erraten oder stehlen können, dadurch ist Phishing passé
- Passkeys werden von den Browsern oder Betriebssystemen berechnet, damit sie nur für den entsprechenden Dienst verwendet werden, anstatt sich auf die Überprüfung durch den Benutzer zu verlassen.
- geräte- und plattformübergreifende Authentifizierung, d. h., eine Anmeldung auf einem fremden Gerät kann durch das eigene Gerät, auf welchem sich der Privat Key befindet, autorisiert werden.

Passkeys im Vergleich zu Kennwörtern

Herkömmliche Passwörter

1. **Textbasierte Zeichenfolgen**:
   Passwörter sind eine Kombination aus Buchstaben, Zahlen und Sonderzeichen, die der Benutzer sich merken muss.
2. **Manuelle Eingabe**: Benutzer müssen Passwörter manuell eingeben, was zeitaufwendig und fehleranfällig sein kann. Eingabeformate (Anzahl Ziffern, Sonderzeichen) etc., sind unterschiedlich
3. **Phishing**: Passwörter können leicht durch Phishing-Angriffe gestohlen und missbraucht werden.
4. **Leaks**: Benutzerdaten und Passwörter können gestohlen werden
5. **Regelmässige Änderungen**:
   viele Systeme verlangen, dass Passwörter regelmässig geändert werden, was für Benutzer umständlich sein kann.

Passkeys

1. **Kryptografische Schlüsselpaare**:
   Passkeys basieren auf einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel wird auf dem Server gespeichert und der private Schlüssel sicher auf dem Gerät des Benutzers verbleibt.
2. **Biometrische Authentifizierung**: Passkeys können mit biometrischen Daten wie Fingerabdruck oder Gesichtserkennung (z.B. über Windows Hello) verwendet werden, um den privaten Schlüssel zu entsperren.
3. **Phishing-Schutz**: Da Passkeys keine wiederverwendbaren Informationen wie Passwörter übertragen, sind sie nicht anfällig für Phishing-Angriffe.
4. **Einfachheit**: Die Authentifizierung erfolgt schnell und sicher über biometrische Daten oder eine PIN.

Passkeys bieten eine sicherere und benutzerfreundlichere Alternative zu herkömmlichen Passwörtern.

Passkeys im iCloud-Schlüsselbund von Apple

Der **iCloud-Schlüsselbund ist der Passwortmanager** in welchem Passkeys und Passwörter, Kreditkarten- und andere Informationen verschlüsselt auf allen autorisierten Applegeräten synchron und aktuell gehalten werden.

Falls noch nicht eingerichtet, auf allen Geräten:
› Einstellungen › [dein Name] › iCloud › Passwörter & -Schlüsselbund
› aktiviere Option iPhone synchronisieren.

Die geräteübergreifende Synchronisierung des iCloud-Schlüsselbunds bietet Komfort und Redundanz bei Verlust eines Gerätes.

Auf Apps/Webseiten die Passkeys anbieten, können diese nun verwendet werden und erlauben das Anmelden mit FaceID oder TouchID .

Passkeys in Google und Anforderung an Plattformen

Passkeys werden im Google Passwortmanager umfassend unterstützt.

Passkeys ermöglichen das Anmelden mit Fingerabdruck, Gesichtserkennung oder PIN im Google-Konto und anderen unterstützten Diensten.

Die Passkeys können auf verschiedenen Betriebssystemen und Browsern verwendet werden, einschliesslich Android, iOS, Windows, macOS und ChromeOS.

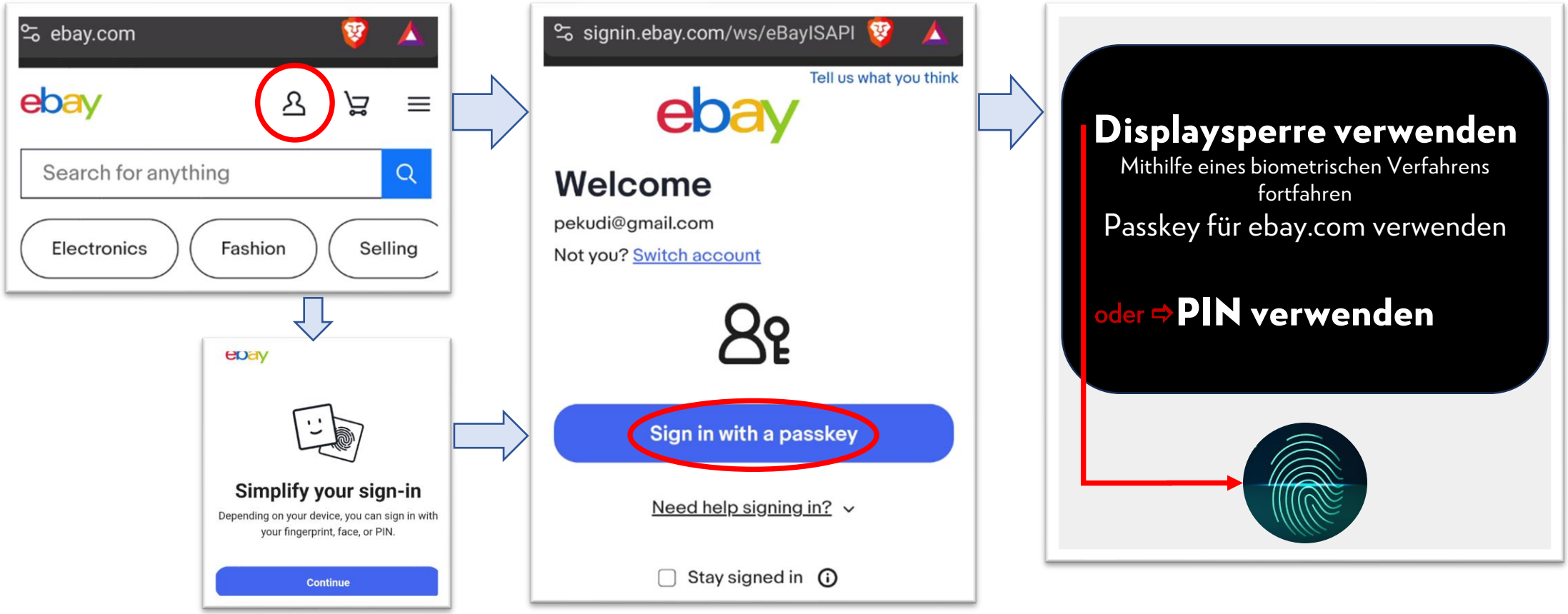
Auf Android-Geräten werden Passkeys im Google Password Manager gespeichert und sicher mit anderen Android-Geräten synchronisiert.

Mindestanforderung für die Unterstützung von Passkeys

Betriebssysteme: ab Windows 10, macOS Ventura, ChromeOS 109, Smartphone ab iOS 16 oder Android 9
Browser: ab Chrome 109, Brave 1.45, Safari 16, Edge 109, FireFox 122,

15 Minuten

Anmelden mit Passkeys auf Smartphone– z.B. ebay.ch



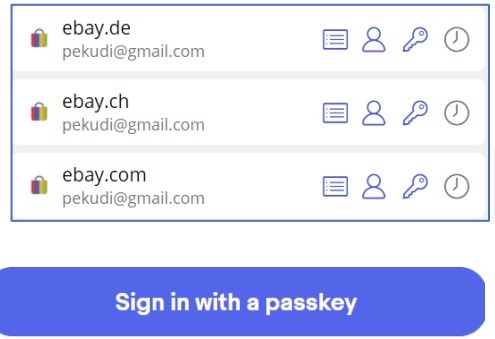
Beispiele mit Passkeys

3 Regionen .de .com und .ch
Login überall mit gleichem Passwort möglich, jedoch pro Region jeweils andere Passkeys nötig.

Ebay.de
Keine Passkeys angelegt.
Login mit Bitwarden Passwort

Ebay.com
Login mit Passkeys

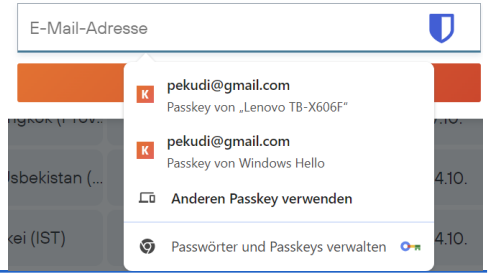
Ebay.ch
Neue Passkeys anlegen
und wieder löschen auf beiden Seiten



Anmelden mit Passwort oder
Passkeys auf anderem Gerät mit QR Code

iPhone, iPad oder Android-Gerät

Anmelden mit Passkeys
mit Windows Hello



Passwortmanager – was ist das?

Ein Passwortmanager ist eine App, die Passwörter und mehr in einem digitalen Tresor speichert.

Der Passwortmanager sollte 2FA „Zweifaktoren-Authentisierung“ unterstützen oder durch ein starkes Masterpasswort geschützt sein.
Wird das Passwort entwendet, erhalten Unbefugte Zugang zu allen gespeicherten Passwörtern.

Es gibt Offline-Lösungen z.B. KeePassXC sowie Online- bzw. Cloud-Passwortmanager:

- **Plattform-Passwortmanager**: iCloud Schlüsselbund, Windows Hello, Google Passwortmanager
- **Browser-Passwortmanager**: Safari, Chrom, Brave
- **Vollwertige Passwortmanager**: Bitwarden, 1Password, Dashline, KeePass etc.
  Alle sind preiswert von kostenlos bis günstige ca. 10.-
  plattformunabhängig
  speichern auch Karten-, ID- und andere Informationen;
  weitere Zusatzdienste wie PW-Analysen, PW teilen, sicheres Senden, Dateispeicherung, Leak-Erkennung …

Passwortmanager – wozu?

Passkeys werden die Passwörter irgendwann ablösen und Passwort- werden zu Passkeys Manager. Dadurch werden sie eher an Bedeutung zunehmen, da sie Geräte und Plattform unabhängig sind.

Die Passwörter/Passkeys sind dabei an eine Anwendung, den Passwortmanager, iCloud-Schlüsselbund oder Windows Hello und nicht mehr nur an ein Gerät gebunden.

Passwortmanager bieten zahlreiche Vorteile:

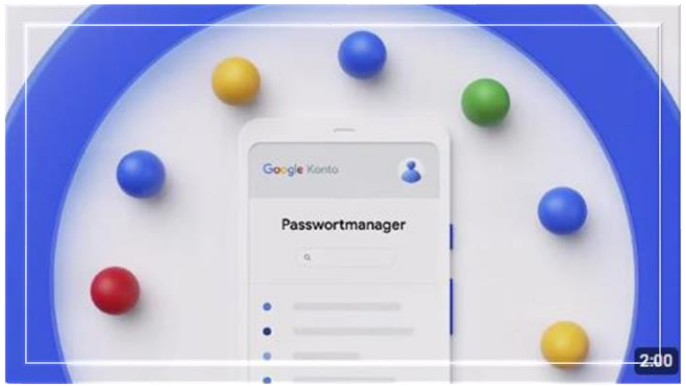
Speicherung:	Die Passwörter werden verschlüsselt, zentral gespeichert und über Geräte und Plattformen hinweg synchronisiert. Der Zugriff auf die Passwortdatenbank erfolgt mit einem Masterpasswort.
Sicherheit:	Passwörter müssen nicht mehr selber erdacht werden, dadurch überall lang, stark, einzigartig für jede Website . Das Risiko von Hackerangriffen und Phishing wird erheblich reduziert
Komfort:	Keine Zettelwirtschaft; automatische starke Passwortgenerierung und automatisches Anmelden.
Zusätzlich:	gute Passwortmanager können auch Kreditkarten- und andere wichtige Informationen aufnehmen. ⇨ das ersetzt ev. die Zugangsliste für den Digitalen Nachlass (siehe Digitreff vom 25.4.2024)

Passwortmanager z.B. von Google

These: Besser geschützt mit einem Passwortmanager als ohne

Funktionen des Google Passwortmanager:

- Generiert starke, nur einmal verwendete Passwörter und speichert diese im Google-Konto, damit man sich diese nicht merken muss.
- Die Passwörter sind mit integrierten Sicherheitsfunktionen geschützt.
- Passwörter auf Websites und in Apps werden automatisch ausgefüllt.



YouTube 2 Min.

https://youtu.be/ieSv9cdHemc?si=_naAnmeuq_JV4R9F

Hinweis:
Die Sicherheit der gespeicherten Passwörter kann erhöht werden, indem Informationen zur Kontowiederherstellung hinzugefügt und die 2-Faktor-Authentifizierung aktiviert werden.

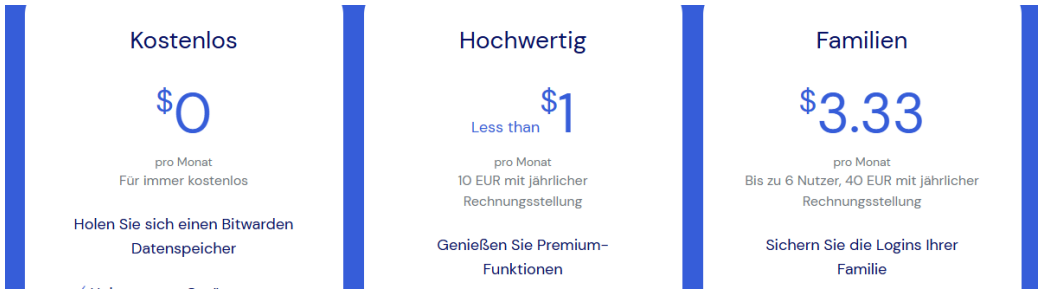
Passwortmanager – welche?

Apple und Google haben ihre eigenen Passwortmanager, die mit Passkeys umgehen können.

Möchte man einen unabhängigen Passwortmanager, so empfehle ich
Zwei die sich beide gut für verschiedene IT-Plattformen eignen:

Bitwarden https://bitwarden.com

Als Open-Source sowohl sicher als auch flexibel.
Benutzerfreundliche Oberfläche.
Fr. 0.- bis 40.- pro Jahr und Familie



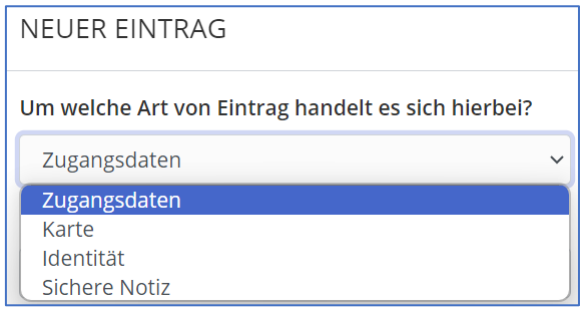
1Password https://1password.com

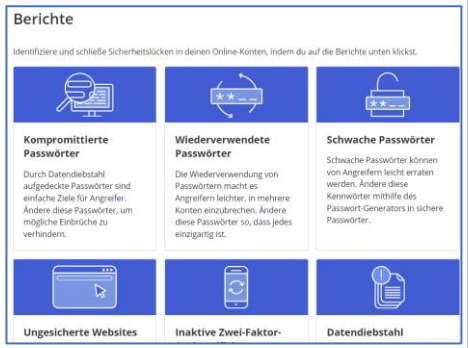
Benutzerfreundlich und kompatibel.
Fr. 36.- bis 60.- pro Jahr und Familie

Passwortmanager – Bitwarden oder 1Password

Bitwarden

https://bitwarden.com

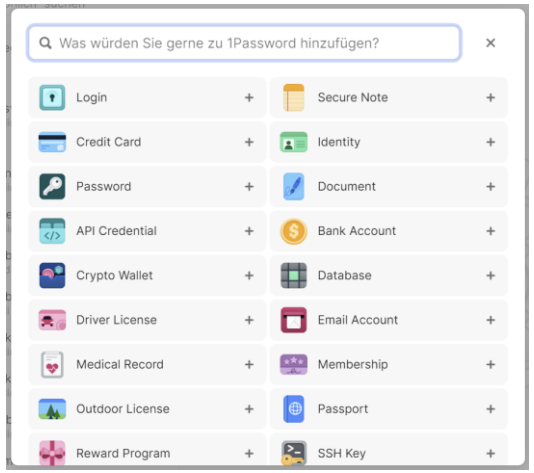




Ist OpenSource.
Berichte umfassender. Passwortgenerator.
Oberfläche etwas altbacken.
Ev. Ist aber Gratisversion genügend.

1Password

https://1password.com



Benutzerfreundlicher, schön gemacht, responsiv.

Gibt es eine Präferenz?

Abschluss

Kurzes Feedback zu diesem DigiTreff

auf Zettel:

Wie hat es dir heute gefallen? 1-6 (1=😢 6=😊)

Welche drei Ideen/Tricks/Tipps/Themen habe ich heute mitgenommen

Danke dass du dabei warst!