Digital Dabei

Sicher im Internet mit einem Passwortmanager

Mit uns Digital im Alter BREMEN-NORD

in Kooperation mit Stadt Bibliothek Bremen

Was wir heute machen

1. Wie Passwörter gestohlen werden
2. Woran man ein gutes Passwort erkennt
3. Der Passwortmanager und welche es gibt
4. Live-Vorführung: So richte ich ihn ein

Fragen dürfen Sie jederzeit stellen.

Bitte melden Sie sich

- Wer benutzt dasselbe Passwort für mehrere Internetseiten?
- Wer hat seine Passwörter auf einem Zettel notiert?
- Wer hat schon einmal ein Passwort vergessen?

Fast alle Hände gehen hoch. Genau deshalb sind wir heute hier.

Wie kommen Betrüger an Passwörter?

- Datenlecks: Eine Firma wird gehackt, und die Passwörter landen im Internet.
- Phishing: Gefälschte E-Mails locken auf falsche Seiten, und Sie tippen das Passwort selbst ein.
- Raten: Programme probieren in kürzester Zeit sehr viele einfache Passwörter aus.

Gefährlich wird es, wenn ein Passwort überall benutzt wird. Ein Leck öffnet dann viele Türen.

Welches Passwort ist am sichersten?

A Schatz1958

B 12345678

C Bello!Bello!

D Mein Hund Bello frisst gern Käse im Garten

Abstimmung per Handzeichen. Die Auflösung kommt gleich.

Das macht ein gutes Passwort aus

- Es ist lang. Ein ganzer Satz ist besser als wilde Sonderzeichen.
- Es gilt nur für ein Konto. Dann öffnet ein gestohlenes Passwort nur eine Tür.
- Es lässt sich nicht erraten: kein Vorname, kein Geburtsdatum, keine Zahlenreihe.

Die Lösung des Quiz: Antwort D.

Der Passwortmanager als Tresor

Stellen Sie sich einen Tresor vor, in dem alle Ihre Passwörter liegen.

Den Schlüssel dazu merken Sie sich: das Master-Passwort.

Alles andere merkt sich der Tresor. Er ist verschlüsselt und lässt sich nur mit Ihrem Schlüssel öffnen.



Quelle: pngimg.com

Was der Passwortmanager für Sie tut

- Er erfindet starke Passwörter für jede Seite.
- Er merkt sich alle Zugangsdaten, verschlüsselt.
- Er trägt sie nur auf der echten Internetseite ein, auf Fälschungen nicht.
- Er warnt, wenn ein Passwort schwach ist oder doppelt benutzt wird.

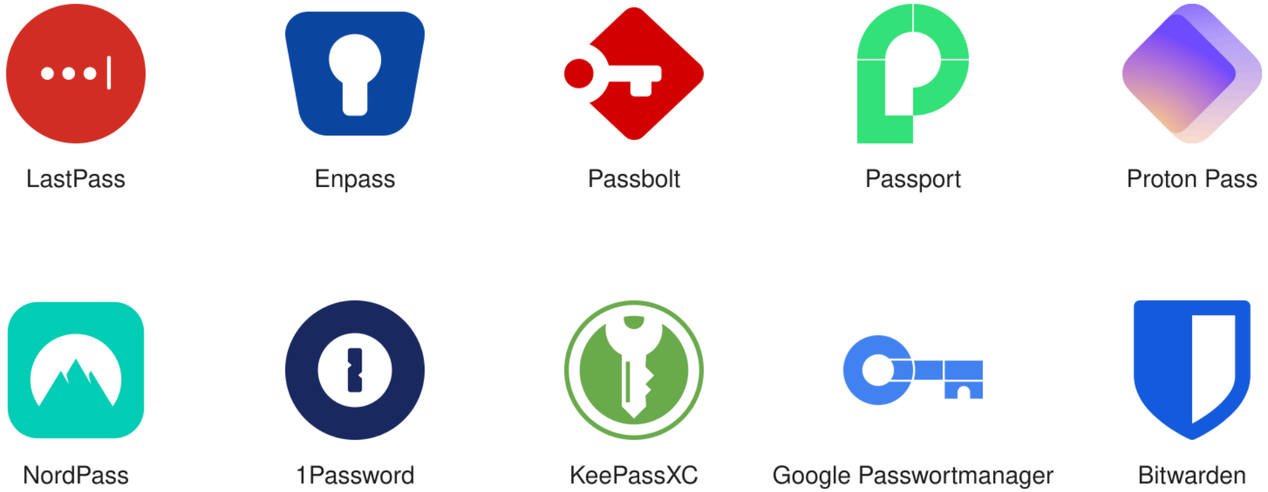
Ist das wirklich sicher?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Passwortmanager. Der Nutzen ist deutlich größer als die Risiken.

- Wählen Sie einen Anbieter, der Ihre Daten nicht selbst lesen kann.
- Liegen die Daten im Internet, fragen Sie, wo sie gespeichert werden und wie sie geschützt sind.
- Nehmen Sie ein starkes Master-Passwort und spielen Sie Updates zeitnah ein.

Quelle: BSI und FZI, Studie zu zehn Passwortmanagern (Dezember 2025)

Die Qual der Wahl



Im Internet gibt es mehr als 50 Passwortmanager

allein kostenlose Anbieter sind es über 30 – dies hier sind 10 davon

Warum europäische Anbieter?

- Es gilt europäisches Datenschutzrecht (DSGVO). Die Schweiz hat ein eigenes Datenschutzgesetz.
- Die Daten liegen auf Ihrem Gerät oder auf Servern in Europa. Bei Bitwarden wählen Sie dafür den EU-Server.
- Viele Programme sind Open Source: Jeder kann prüfen, was sie tun.

Die Schweiz gehört nicht zur EU, ist aber ein europäisches Land.

Europäische Passwortmanager im Überblick

Name	Herkunft	Kosten
KeePassXC	Gemeinschaftsprojekt	Kostenlos, Daten nur auf Ihrem Gerät
Proton Pass	Schweiz	Kostenlos, Plus ab ca. 3 $ im Monat
Bitwarden	Firma in den USA, Server in der EU wählbar	Kostenlos, Premium ca. 20 $ im Jahr
Padloc	Deutschland	Open Source, Tarife vorab prüfen
Bitdefender SecurePass	Rumänien	Nur kostenpflichtig

Stand: Recherche November 2026. Preise und Tarife bitte vor dem Vortrag auf den Webseiten der Anbieter prüfen.

Mit uns Digital im Alter BREMEN-NORD in Kooperation mit Stadt Bibliothek Bremen

Gut zu wissen: Diese sind nicht europäisch

USA und Kanada

- 1Password (Kanada)
- LastPass, Keeper, Norton, McAfee (USA)

Große Techkonzerne

- Google: Passwörter im Chrome-Browser
- Apple: Schlüsselbund
- Microsoft: Passwörter im Edge-Browser

Bequem, aber an einen Konzern gebunden. Deshalb stellen wir sie heute nicht in den Mittelpunkt.

Mein Eindruck nach der Recherche: Proton Pass

- Der Anbieter sitzt in der Schweiz.
- Kostenlos, mit unbegrenzt vielen Passwörtern und Geräten.
- Läuft am Computer und am Handy.
- Warnt vor schwachen und doppelten Passwörtern.

Eine Alternative ist KeePassXC. Dort bleibt alles auf Ihrem Computer, es braucht aber etwas mehr Technik.

Der Gratis-Tarif reicht für Passwörter. Zusatzfunktionen wie Passwort-Teilen oder Überwachung kosten Geld.

Persönlicher Eindruck nach eigener Recherche, keine Empfehlung oder Zusicherung. Angaben ohne Gewähr, Nutzung auf eigene Verantwortung.

Live: So richte ich ihn ein

1. Kostenloses Konto bei Proton Pass anlegen
2. Master-Passwort als langen Satz ausdenken
3. Wiederherstellungsdaten ausdrucken und verwahren
4. Browser-Erweiterung oder Handy-App installieren
5. Erstes Passwort speichern und automatisch einfügen lassen

Ich zeige es live auf der Leinwand. Zu Hause können Sie es in Ruhe nachmachen, das Handout hilft dabei.

Das Master-Passwort

Es ist der eine Schlüssel zum Tresor, am besten ein langer Satz.

Zitat: „Wage es, weise zu sein“ (Horaz, um 20 v. Chr.) und dazu Ihr Zusatz: „auch mit 70!“

So sieht das Passwort dann aus:

```
Wage es, weise zu sein (Horaz, um 20 v. Chr.) auch mit 70!
```

- Niemals weitergeben, nicht am Telefon und nicht per E-Mail.
- Notfallblatt: einmal aufschreiben und zu Hause im Umschlag aufbewahren.
- Wo möglich Zwei-Faktor einschalten, vor allem bei E-Mail und Bank.

Drei Wege zum Master-Passwort

1. Fünf bis sechs zufällige Wörter, die nichts miteinander zu tun haben

`Tisch Lampe Wolke Kaffee Bremen Fenster`

2. Ein Zitat mit Zahlen und Zeichen mitten im Satz

`Wer-rastet,-der-rostet!-2026-in-Lesum`

3. Ein schönes Erlebnis mit Datum und Uhrzeit

`Am 14.6.2009 um 17:30 Uhr gab es Eis am Weserdeich!`

Mindestens 25 Zeichen, möglichst ohne Umlaute und ß. Diese Beispiele bitte nicht übernehmen.

Was ist Zwei-Faktor?

Wie am Geldautomaten: Sie brauchen die Bankkarte und die PIN.

1. Sie geben Ihr Passwort ein.
2. Dann kommt ein Code auf Ihr Handy, per SMS oder aus einer App.
3. Den Code geben Sie auch ein. Erst dann sind Sie angemeldet.

Ein Dieb, der nur Ihr Passwort kennt, kommt nicht hinein. Besonders wichtig bei E-Mail-Konto und Online-Banking.

Fünf Regeln zum Mitnehmen

1. Für jedes Konto ein eigenes Passwort.
2. Lang ist besser als kompliziert, ein Satz genügt.
3. Der Passwortmanager merkt sich alles für Sie.
4. Das Master-Passwort aufschreiben und zu Hause verwahren, aber nie weitergeben.
5. Am Telefon oder per E-Mail darf niemand Ihr Passwort verlangen.

Jetzt sind Ihre Fragen dran.

Später fragen: hallo@dia-bremen.de · dia-bremen.de