Enpass Test: Das bietet der Passwort-Manager

Datum: 06.05.2019 | Datenschutz, Sicherheit, Softwaretests

Email, Social Media oder Online-Banking: **Im Internet geht heutzutage nichts mehr ohne Login-Daten** und genau da liegt auch das Problem. Durch schlecht gesicherte Kennwörter **können Sie nämlich ganz schnell zum Opfer von Daten- oder Identitätsdiebstahl werden**. Abhilfe schafft ein Passwort-Manager, mit dem Sie Ihre **Zugangsdaten und Kennwörter besser schützen und organisieren** können. Das kostenlose Tool Enpass bietet eine Reihe nützlicher Features und punktet nicht zuletzt durch einen attraktiven Preis. Wir haben den Enpass Passwort-Manager **einem ausgiebigen Test unterzogen** und zeigen, wie er sich in der Praxis schlägt.

- ✔ Für die Kodierung verwendet Enpass 256-Bit-AES und verschlüsselt die Daten zusätzlich über 100 000 PBKDF2-HMAC-SHA512-Runden mit SQLCipher.
- ✔ Enpass betreibt keine Cloud, sondern speichert die Passwort-Datei lokal auf dem Rechner des Nutzers ab.
- ✔ Für die Nutzung von Enpass fallen keine Abo-Gebühren an. Die Lizenz (für die Pro-Version) muss nur einmal erworben werden und ist im Anschluss ein Leben lang gültig.

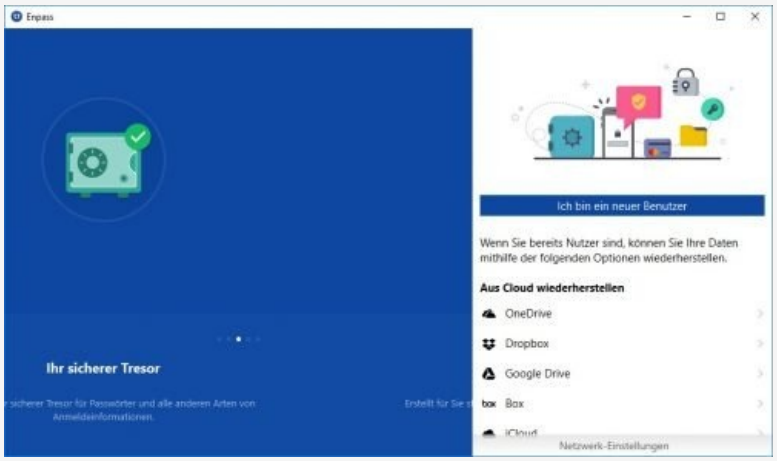
Inhalt [Ausblenden]

1. Installation und Einrichtung des Enpass Passwort-Managers

Im Gegensatz zu vielen anderen Passwortmanagern (z.B. KeePass oder LastPass) **gibt es bei Enpass keine Online-Benutzerkonten**, die Nutzung der Software erfolgt ausschließlich lokal**.** Erfreulicher Weise ist **für den Download auch keine Registrierung beim Hersteller erforderlich**. Auf der offiziellen Download-Seite finden Sie neben der Desktop-Version zum Speichern Ihrer Passwörter auch das Browser-Plugin, das diese automatisch in die Anmeldeformulare von Internetseiten einträgt.

Enpass kann plattformübergreifend (auf Windows, Linux oder MacOS) eingesetzt werden und berücksichtigt dabei auch die mobilen Betriebssysteme. Das Browser-Plugin ist für Chrome, Firefox, Edge, Safari und Opera verfügbar.

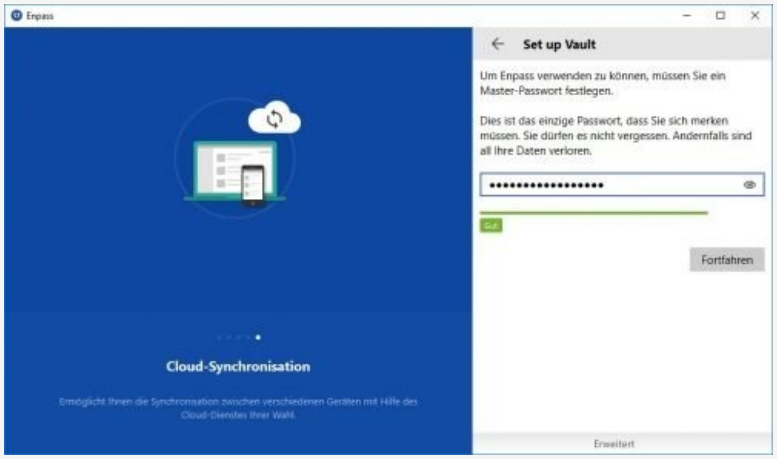
Die Installation auf unseren Windows 10-Notebook verlief ziemlich unkompliziert: Der Assistent kommt ohne großes TamTam aus. Nach dem Herunterladen aus dem Microsoft Store (der offizielle Download-Link hat uns dorthin umgeleitet) wurde das Programm automatisch installiert und direkt im Anschluss daran geöffnet.



Enpass möchte als Erstes wissen, ob Sie ein neuer Benutzer sind.

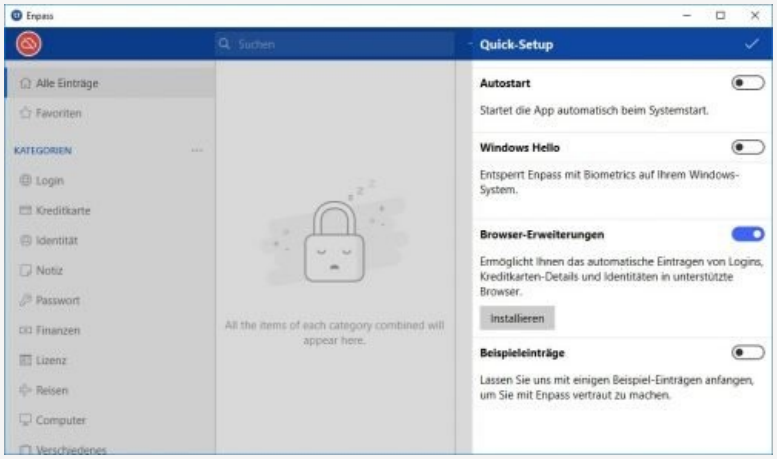
Nach dem Start fragt Enpass Sie als erstes, ob Sie ein neuer Benutzer sind, oder Ihre **Daten einer Sicherung wiederherstellen** möchten. Wir nutzen das Programm für unseren Test zum ersten Mal, daher klicken wir hier auf „**Ich bin ein neuer Benutzer**“.

Als Nächstes werden Sie gebeten, **ein Masterpasswort festzulegen**. **Wählen Sie hier immer ein besonders starkes Passwort**, dass den Richtlinien für sichere Passwörter entspricht, da es zukünftig den Zugang zu Enpass sowie alle darin gespeicherten Daten schützt. Geben Sie das gewählte Passwort im drauffolgenden Fenster zur Bestätigung erneut ein und klicken Sie auf „Weiter“.



Legen Sie Ihr Masterpasswort auf Basis der geltenden Regeln für sichere Passwörter fest.

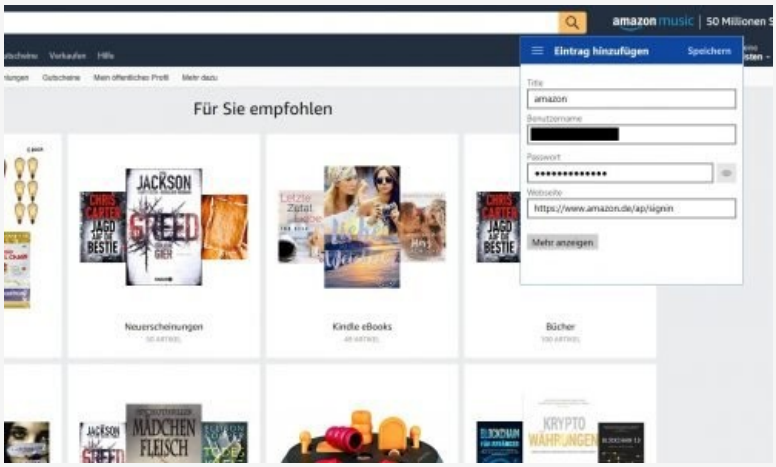
Wir befinden uns nun bereits im Inneren der Passwort-Bibliothek. Auf der rechten Seite wird das Quick-Setup-Menü eingeblendet, in dem Sie zum Beispiel **Browser-Erweiterungen installieren oder einen Autostart-Eintrag für Enpass erstellen** können. Sämtliche Einstellungen können Sie aber natürlich auch nachträglich noch anpassen.



Über das Quick-Setup können Sie die wichtigsten Konfigurationen "on the fly" erledigen.

2. Passwörter verwalten und speichern mit dem Enpass Passwort-Manager

Das Speichern von Passwörter funktioniert mit Enpass analog zu den meisten anderen Passwort-Managern: **Wenn Sie sich mit Ihren Zugangs-Daten anmelden, fragt das Programm, ob diese gespeichert werden sollen**. Sie können den Vorschlag natürlich auch jederzeit über die Optionen „**nie für diese Seite**“ oder „**nicht jetzt**“ ablehnen.



Nach einmaligem Speichern trägt Enpass die Daten beim Aufruf einer Login-Seite ab sofort automatisch ein.

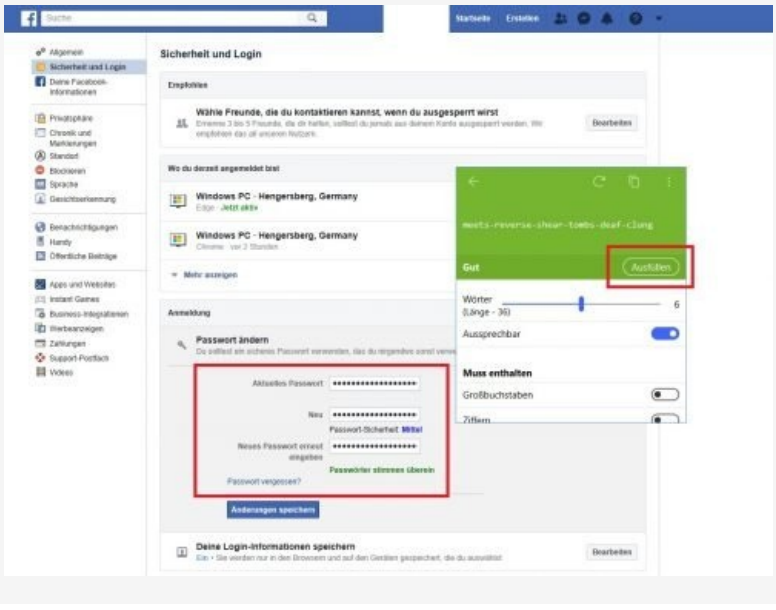
Einmal gespeichert, trägt Enpass beim Aufruf einer Login-Seite ab sofort **automatisch die entsprechenden Daten** für Sie ein. Dazu müssen Sie lediglich den entsprechenden Eintrag mit einem Doppelklick auswählen. Anschließend trägt Enpass die Daten in die vorgesehen Felder ein und sendet die Anfrage direkt ab.

Ein bereits gespeichertes Passwort können Sie in Enpass auf zweierlei Arten aktualisieren: Entweder, Sie gehen in der Anwendung auf den entsprechenden Eintrag und ändern das Passwort direkt dort ab, oder Sie nutzen das Browser-Plugin und den Passwort-Generator.

In unserem Test möchten wir unser Facebook-Kennwort ändern und es gleich in Enpass übernehmen. Dazu gehen wir im ersten Schritt auf die Seite mit den Kontoeinstellungen und navigieren dort unter „**Sicherheit und Login**“ und klicken beim Unterpunkt „**Anmeldung -> Passwort ändern**“ auf „**Bearbeiten**“.

Über "Sicherheit und Login" können Sie in Facebook ihre Passwort-Einstellungen anpassen.

Nach einem Klick auf die Browser-Erweiterung bietet uns der Passwort-Manager den passenden Eintrag mit unseren Login-Daten an. **Um das Kennwort zu ändern, klicken wir links unten auf den Passwort-Generator** (das Pfeil-Symbol mit dem Stern in der Mitte).



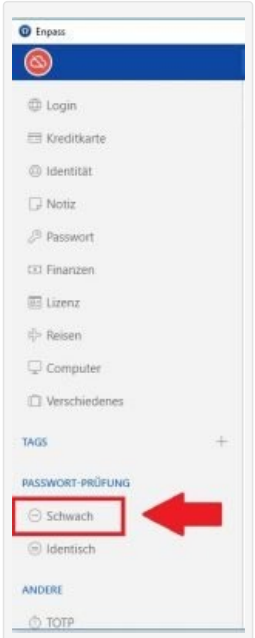
Die Daten aus Enpass werden automatisch in Facebook-Maske übernommen.

Im Anschluss können wir Länge und Komplexität unseres neuen Kennwortes festlegen. Mit einem Klick auf „**Ausfüllen**“ werden die Daten in die Facebook-Maske eingetragen und können dort anschließend über den Button „**Änderungen speichern**“ übernommen werden. Zugleich wird der hinterlegte Wert **auch in Enpass aktualisiert**.

2.1. Mehr Sicherheit mit der Passwort-Prüfung

Enpass verfügt über einen integrierten Passwort-Audit, mit dem Sie schwache, veraltete oder doppelte Kennwörter aufspüren und im Anschluss mit Hilfe des Kennwort-Generators durch starke und einzigartige Phrasen ersetzen können. Der Scan unterstützt Sie bei der regelmäßigen Überprüfung und warnt Sie auf Wunsch auch **rechtzeitig vor ablaufenden Passwörtern**.

Um alle schwachen Passwörter zu identifizieren, klicken Sie auf der Seitenleiste unter „**Passwort-Prüfung**“ auf den Eintrag „**Schwach**“. Eine Liste der Elemente mit doppelten Passwörter finden hingegen unter dem Eintrag „**Identisch**“.



Enpass im Test: Über die Passwort-Prüfung findet der Passwort-Manager schwache oder doppelte Kennwörter.

Enpass kategorisiert Ihre Kennwort zudem nach dem Alter und teilt diese dabei in die Kategorien

- mehr als 3 Jahre alt
- 1 bis 3 Jahre alt
- 6 bis 12 Monate alt
- 3 bis 6 Monate alt

ein. **Sie haben außerdem die Möglichkeit, Ihre Kennwörter mit einem Ablaufdatum zu versehen**. Klicken Sie dazu auf das Passwortfeld im betreffenden Eintrag und geben Sie die gewünschte Anzahl von Tagen ein. Die Passwörter, die in einem Tag, einer Woche oder einem Monat ablaufen, werden unter „**Ablaufend am**“ angezeigt.

Tipp: Um bestimmte Kennwörter von der Überprüfung auszuschließen, klicken Sie rechts auf den Eintrag (unter „**Schwach**“ oder „**Identisch**“ und wählen Sie „**Von Passwort-Prüfung ausschließen**“. Ausgenommene Kennwörter erscheinen dann nicht mehr in den Ergebnislisten.

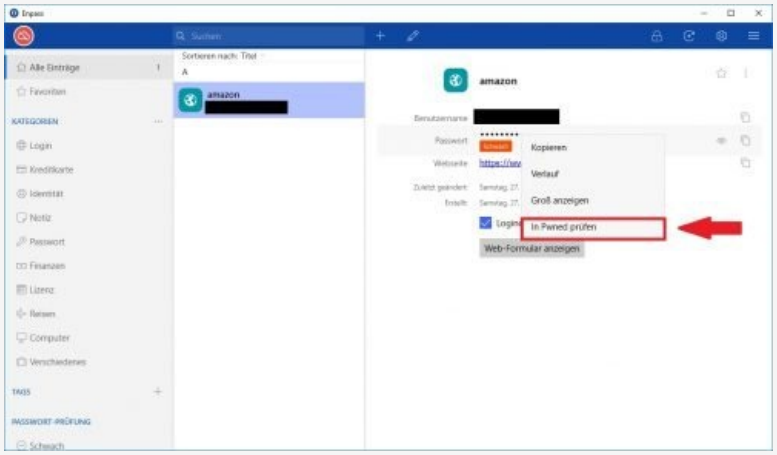
2.2. „Pwned Passwords“ findet gehackte Kennwörter

Seit der Version 5.6.8 können Sie in Enpass auch überprüfen, **ob die von Ihnen verwendeten Kennwörter schon einmal gehackt oder gestohlen wurden**. Dazu verwendet das Programm die API des Web-Tools Pwned Passwords des australischen Sicherheitsforschers Troy Hunt.

Für den Abgleich stehen über eine halbe Milliarde Datensätze aus Passwortlisten von Hacker-Angriffen und diversen Datenlecks zur Verfügung.

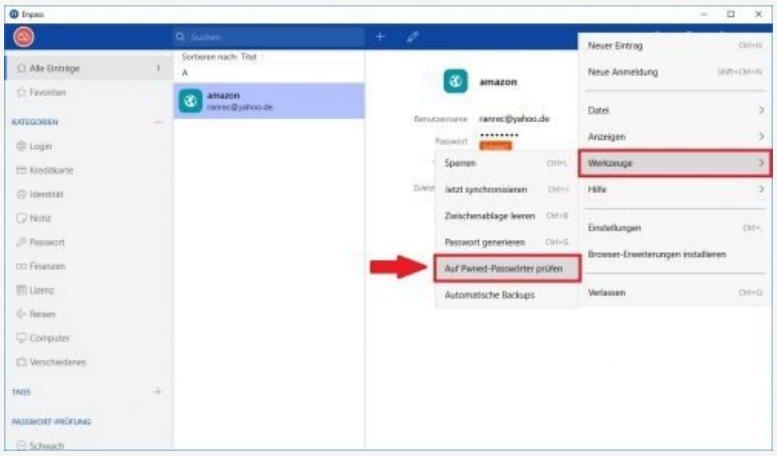
Beachten Sie dabei aber: Landet Pwned Passwords bei Ihrem Kennwort keinen Treffer, bedeutet das nicht automatisch, dass es auch sicher ist.

Um ein einzelnes Passwort in Enpass zu prüfen, klicken Sie mit der rechten Maustaste auf das Kennwort-Feld und wählen „**In Pwned prüfen**“ aus.



Mit "Pwned Passwords" können Sie überprüfen, ob Ihr Kennwort in der Vergangenheit schon einmal gehackt wurde.

Möchten Sie stattdessen sämtliche Kennwörter in der gesamten Datenbank prüfen, klicken Sie im Menü auf „**Werkzeuge -> Auf Pwned-Passwörter überprüfen**“.



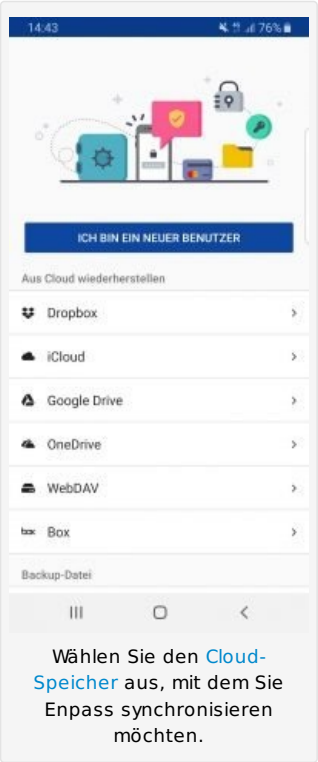
Über die Werkzeuge können Sie auch alle Passwörter auf einmal überprüfen lassen.

Gut zu wissen: Alle Kennwörter, die von Pwned Passwords aufgespürt wurden, zeigt Enpass in der Passwort-Prüfung unter dem Eintrag „**Schwach**“ an.

2.3. Mobile Nutzung mit der Enpass-App im Test

Um den Enpass Passwort-Manager auch mobil nutzen zu können, müssen Sie eine Verbindung mit einem Cloud-Speicher (z.B. Dropbox, Google Drive oder Microsoft OneDrive) **herstellen** und die Daten der Desktopversion darüber snychronisieren.

Die Enpass-App ist für Android, iOS oder Windows Phone verfügbar, **die Zahl der Einträge ist bei den kostenlosen Mobilversionen aber auf maximal 20 begrenzt**. Wem das nicht reicht, für den besteht die Möglichkeit, auf den „**Enpass Password Manager Pro**“ upzugraden. Für unserem Test haben wir die Android-Variante auf einem Samsung Galaxy S9 installiert.



Wählen Sie den Cloud-Speicher aus, mit dem Sie Enpass synchronisieren möchten.

Nach der Auswahl des Cloud-Speichers mussten wir lediglich bestätigen, dass Sie wir **dem Passwort-Manager die erforderlichen Zugriffe gewähren**. Im Anschluss wurden sofort alle Einträge automatisch von der App synchronisiert.

3. Preise und Verfügbarkeit des Passwort-Managers

Die Basis-Version von Enpass gibt es als kostenlosen Download, sie ist allerdings bei Mobilgeräten auf 20 Einträge begrenzt (Desktop: unlimitiert) und **kann jeweils nur auf einem Engerät genutzt werden**. Für einmalig 11,99 USD (10,74 Euro) erhalten Sie mit der **Premium Version** hingegen nicht nur **eine Lizenz auf Lebenszeit** (für ein Endgerät): In der mobilen Version können Sie darüber hinaus unlimitierte Mengen an Passwörtern speichern. Die Premiumversion für den Desktop bietet zusätzlich die Möglichkeit, Windows Hello oder Touch ID zu nutzen und Kategorien und Vorlagen des Passwort-Manages zu personalisieren.

Gute Nachricht für Linux-Nutzer: In der kostenlosen Version für Linux-Systeme sind alle Premium-Features bereits erhalten.

4. Fazit unseres Enpass-Test: Guter Passwort Safe zu einem günstigen Preis

Im Gegensatz zu den meisten anderen Alternativen betreibt Enpass keine eigene Cloud und **beschränkt sich auf einen lokalen Betrieb**. Aus diesem Grund verzichtet der Hersteller auch auf den Einsatz von Nutzerkonten. Dennoch bietet der Passwort-Manager zahlreiche praktische Funktionen und erlaubt **neben Login-Daten auch das Anlegen weitere Eintragstypen wie Kontodaten, Finanzen oder Reiseterminen**.

In der Basis-Version kann Enpass ohne Einschränkungen dauerhaft kostenlos genutzt werden, **für die Pro-Varianten wird eine einmalige Zahlung von 11,99 USD fällig**. Dafür ist die Lizenz dann aber auch auf Lebenszeit gültig. Alles in allem präsentierte sich Enpass in unserem Test als **solider Passwort-Manager**, den wir durchaus weiterempfehlen können.

Vorteile

- ✔ Für zahlreiche Plattformen verfügbar
- ✔ In der Basis-Version kostenlos
- ✔ Lizenz ist auf Lebenszeit gültig
- ✔ Integrierte Passwortüberprüfung und Pwned Passworts
- ✔ Viele verschiedene Eintragstypen möglich

Nachteile

- ✘ externer Cloudspeicher notwendig (für Synchronisation auf mehreren Geräten)
- ✘ Formular-Erkennung arbeitet nicht immer astrein

45 Bewertungen

Ø 4,58

Ähnliche Artikel:

- Dashlane-Test: Wie gut ist der Passwort-Manager?
- Avast Test 2019: Wie schlägt sich die Internet…
- USB-Stick-Schlüssel: Die bequeme Art, Ihren PC zu schützen
- Sicherheit im Heimnetzwerk – so schützen Sie Ihren…
- Download der Woche 20/17: BoxCryptor Desktop
- Xiaomi Mint Browser: Diese Features bietet der neue…