

Mehr Sicherheit durch Passwortmanager

Michael Georg Schmidt

Ein Beitrag der studentischen Gruppe ITS Us.
der TH Lübeck.

8. August 2023



Zusammenfassung

Dieser Artikel erklärt Ihnen was *Passwortmanager* sind, und warum Sie einen nutzen sollten. Er erklärt Ihnen auch den Unterschied zwischen *lokalen* und *online* Passwortmanagern. Weiterhin, wie Sie sie benutzen.

Inhaltsverzeichnis

1	Warum sollte ich einen Passwortmanager nutzen?	3
2	Was ein sicheres Passwort ausmacht	3
3	Lokale und online Passwortmanager	4
3.1	Lokale Passwortmanager	4
3.2	Online Passwortmanager	4
4	Lokaler Passwortmanager - KeePassXC	4
4.1	KeePassXC für automatisches Ausfüllen im Browser nutzen	4
4.2	KeePassXC in Betrieb nehmen	7
4.3	KeePassXC erstellt auch Passwörter	12
5	Online Passwort-Manager Proton Pass	13
5.1	Proton Pass in Betrieb nehmen	13
6	Quellen	15

Präambel

Die Gleichberechtigung aller Geschlechter ist mir uneingeschränkt wichtig. Um diesen Text besser lesbar zu gestalten, verwende ich jedoch nur eine Geschlechtsform.

In diesem Artikel stelle ich zwei Passwortmanager vor - *KeePassXC* und *Proton Pass*. Diese beiden habe ich gewählt, weil ich sie für empfehlenswert halte. Das heißt jedoch *nicht*, dass es nicht noch andere empfehlenswerte Passwortmanager gibt.

Die hier vorgestellten Passwortmanager sind *Open Source*. Ihr Programmcode ist also von jedermann einsehbar. Somit kann jeder nachvollziehen, was die Programme machen, und es sind keine bösen Überraschungen zu erwarten.

1 Warum sollte ich einen Passwortmanager nutzen?

Passwörter sichern den Zugang zu unseren online Konten. Sie sollen *sicher* sein. *Jedes Konto* muss *ein eigenes* Passwort haben.

Da es schwer ist, sich viele, sichere Passwörter zu merken, ist es wichtig einen *Passwortmanager* zu verwenden, denn dann muss man sich nur noch *ein* Passwort merken - das, um den Passwortmanager zu öffnen. Alle anderen Passwörter sind sicher verschlüsselt im Passwortmanager verwahrt.

2 Was ein sicheres Passwort ausmacht

Ein sicheres Passwort sollte folgende Kriterien erfüllen

- GROSSBUCHSTABEN
- kleinbuchstaben
- Ziffern 0...9
- Sonderzeichen @!?'<>'... verwenden
- es sollte möglichst laaaaaang sein, mindestens 16 Zeichen

Am wichtigsten ist es, dass ein Passwort lang ist, denn das bremst die Berechnung eines Passwortes aus. Dann kann ein *sicheres* Passwort auch gern ein Leben lang zum Einsatz kommen.

3 Lokale und online Passwortmanager

Bei Passwortmanagern unterscheidet man zwischen *lokalen* und *online* Passwortmanagern.

3.1 Lokale Passwortmanager

Lokale Passwortmanager haben den *Vorteil*, dass sie nur von Personen, die Zugriff auf das Gerät haben, auf dem sie installiert sind, angegriffen werden können. Damit ist der Kreis der potentiellen Angreifer eher klein.

Der *Nachteil* an lokalen Passwortmanagern ist, dass man sie nur auf dem Gerät nutzen kann, auf dem sie installiert sind. Also muss man für PC, Tablet und Smartphone drei Passwortmanager pflegen.

3.2 Online Passwortmanager

Online Passwortmanager haben den *Vorteil*, dass man sie von allen Geräten, die einen online Zugang haben, nutzen kann.

Gleichzeitig ist dies auch ein *Nachteil*, weil somit jeder, der einen online Zugang hat, versuchen kann den eigenen Passwortmanager anzugreifen.

4 Lokaler Passwortmanager - KeePassXC

KeePassXC können sie hier aus dem Internet herunterladen. KeePassXC gibt es originär nicht für Mobilgeräte.

Um KeePassXC zu installieren, klicken Sie doppelt auf die heruntergeladene Datei und befolgen Sie die Anweisungen zur Installation.

4.1 KeePassXC für automatisches Ausfüllen im Browser nutzen

Um *KeePassXC* mit dem Browser nutzen zu können, müssen Sie noch ein entsprechendes Add-on für Ihren Browser installieren. Für *Firefox* benötigen Sie *KeePassXC-Browser*. Auch für *Chrome* gibt es dieses Add-on. Für *Firefox* erkläre ich die Installation beispielhaft. In *Chrome* sieht sie vermutlich sehr ähnlich aus.

Klicken Sie auf den Button *Zu Firefox hinzufügen*.



KeePassXC-Browser von KeePassXC Team

⚠ Dieses Add-on wird von Mozilla nicht aktiv auf seine Sicherheit überwacht. Stellen Sie sicher, dass Sie ihm vertrauen, bevor Sie es installieren.

[Weitere Informationen](#)

Official browser plugin for the KeePassXC password manager
(<https://keepassxc.org>).

Zu Firefox hinzufügen

Abbildung 1: KeePassXC in Firefox integrieren

Anschließend bestätigen Sie die folgende Maske mit **Hinzufügen**.

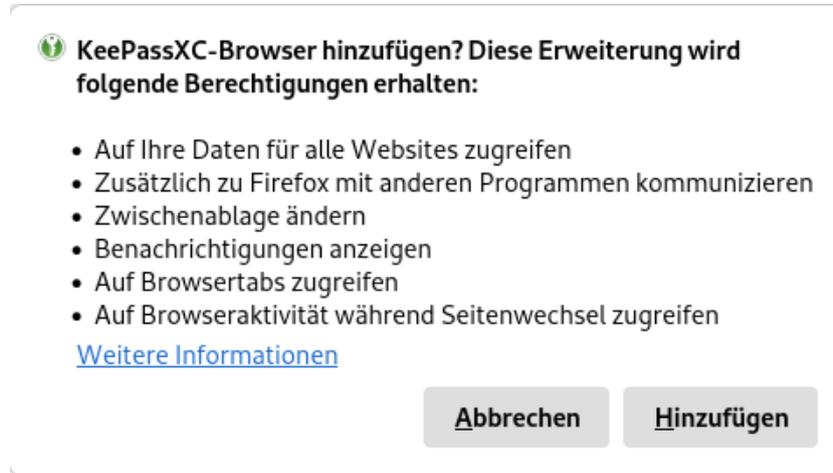


Abbildung 2: Bestätigen Sie mit einem Klick auf **Hinzufügen**

Im nun folgenden Fenster sollten Sie ein Häkchen vor dem Eintrag **Ausführen der Erweiterung in privatem Fenster erlauben** setzen und auf **OK** klicken. Für den Screenshot hat sich dieses Häkchen immer wieder selbst deaktiviert. Nehmen Sie sich kein Beispiel daran ;-).

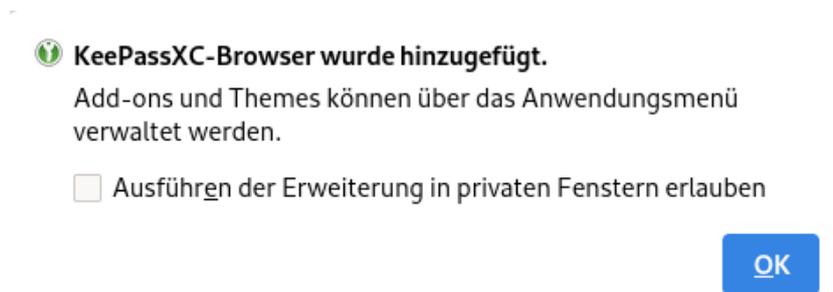


Abbildung 3: Hier sollten Sie ein Häkchen setzen

Das war es schon. Jetzt ist KeePassXC-Browser installiert.

4.2 KeePassXC in Betrieb nehmen

Ihr neu installiertes **KeePassXC** erkennen Sie an dem Logo mit dem weißen Schlüssel im grünen Kreis. Klicken Sie doppelt darauf, um KeePassXC zu starten. Es öffnet sich anschließend eine Maske, mit deren Hilfe Sie eine Datenbank erstellen können, in der Sie Ihre Passwörter und alles, was sicher verwahrt sein soll, speichern können.

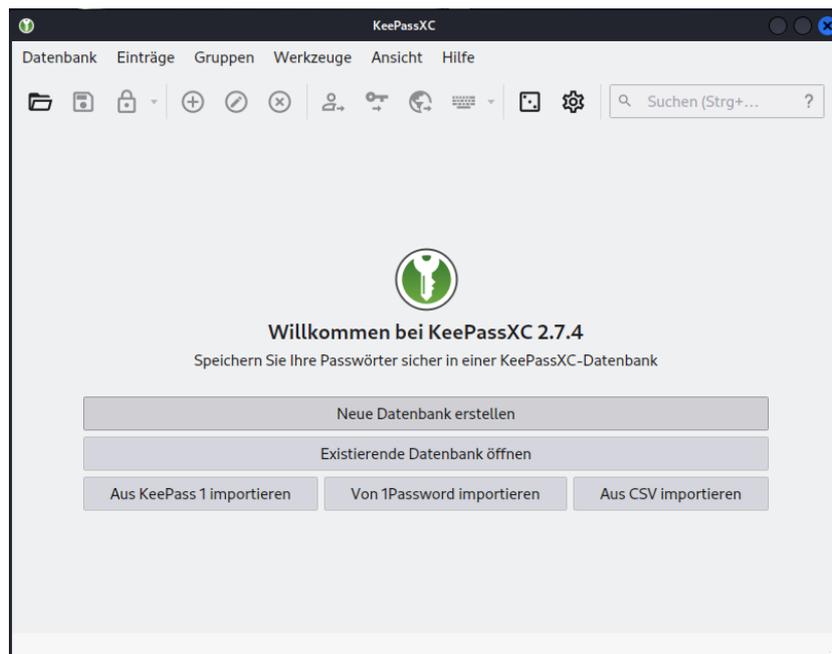


Abbildung 4: Die Startmaske von KeePassXC

Klicken Sie auf *Neue Datenbank erstellen* um die folgende Maske angezeigt zu bekommen.

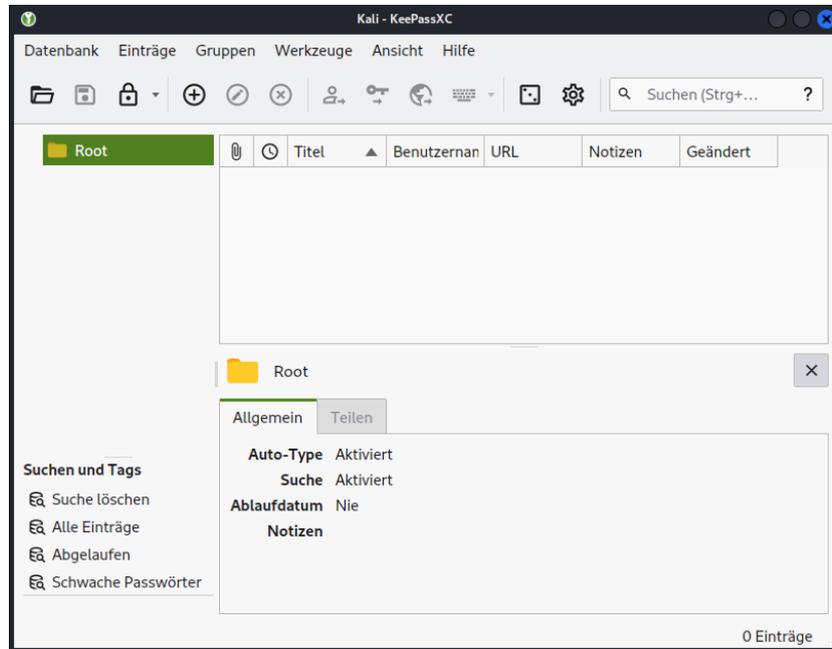


Abbildung 5: KeePassXC Datenbank

Um einen *Ordner* anzulegen, der sich in KeePassXC *Gruppe* nennt, klicken Sie mit der *rechten Maustaste* auf den obersten Eintrag in der linken Spalte der Maske (*Root*) und klicken auf *Neue Gruppe*. Damit können Sie Ihre Passwörter bestimmten Themen zuordnen wie *Webmail*, *Banking* oder *Shopping* oder natürlich beliebigen anderen Bereichen Ihrer Wahl.

Um ein Passwort zu speichern klicken Sie auf das *Plus im Kreis* in der oberen Symbolleiste. Füllen Sie die Maske aus und speichern Sie Ihre Einträge mit einem Klick auf *Ok*.

Wichtig ist hierbei, dass Sie in das Feld *URL* die Internetadresse (URL) der Seite kopieren, auf der Sie sich anmelden wollen, damit KeePassXC später weiß, welches Passwort wohin gehört.

Jetzt ist KeePassXC fast fertig eingerichtet. Es fehlt nur noch ein Schritt. Klicken Sie in der oberen Menüleiste von KeePassXC auf den Eintrag *Werkzeug* und hier auf den untersten Eintrag *Einstellungen*.

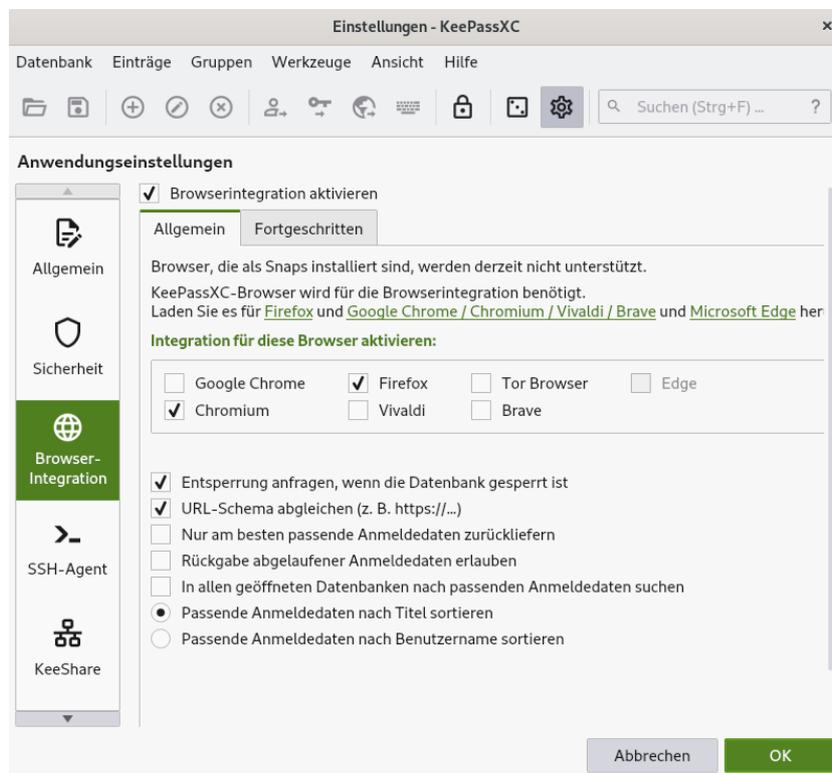


Abbildung 6: Hier wählen Sie Ihren Browser

Hier wählen Sie auf der linken Seite den Eintrag **Browserintegration** und wählen „Ihren“ Browser mit einem Häkchen aus. Jetzt können Sie bei den weiteren Punkten ein Häkchen setzen, wo Sie es für angebracht halten. Abschließend bestätigen Sie Ihre Auswahl mit **OK**.

Nun müssen Sie Ihren Browser mit KeePassXC verbinden. Das machen Sie indem Sie **oben rechts** in der Menüleiste von Firefox auf das Symbol für **Erweiterungen** klicken. Es öffnet sich eine Maske, die alle Ihre installierten Erweiterungen anzeigt. Klicken Sie dieses Symbol an



Abbildung 7: Das Icon zur Anzeige Ihrer Add-ons

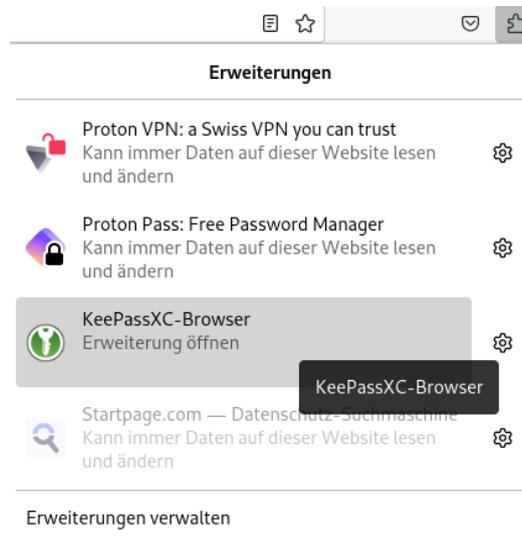


Abbildung 8: Wählen Sie KeePassXC

Wählen Sie hier den Eintrag von KeePassXC.
Anschließend sehen Sie eine Maske bei der Sie nur auf den Button **Verbinden** klicken.

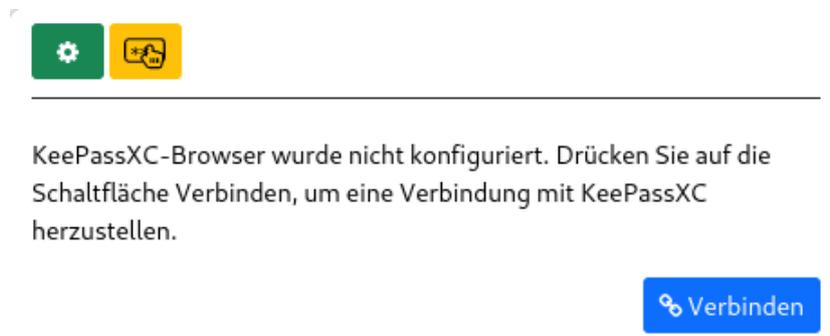


Abbildung 9: KeePassXC mit dem Browser verbinden

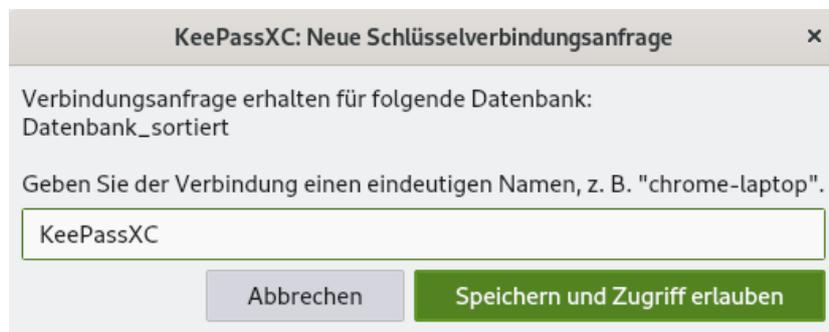


Abbildung 10: Der letzte Schritt

In der abschließenden Maske geben Sie der Verbindung einen Namen. Das kann gerne ***KeePassXC*** sein.

Ab jetzt können Sie ***KeePassXC*** nutzen, um sich automatisch auf Websites anzumelden. Wenn Sie eine Website aufrufen, bei der Sie sich anmelden sollen, sehen Sie folgendes Bild, sofern Sie Ihre E-Mailadresse dafür benötigen. Ansonsten sieht die Maske entsprechend aus - mit dem KeePassXC-Symbol am rechten Rand der Eingabemaske.

E-Mail-Adresse oder Benutzername



Abbildung 11: Ein Klick auf das KeePassXC-Symbol reicht

Klicken Sie auf das KeePassXC-Symbol und Ihre Daten werden eingetragen. Wiederholen Sie diesen Vorgang, bis alle Anmeldefelder ausgefüllt sind und klicken abschließend die Bestätigung.

4.3 KeePassXC erstellt auch Passwörter

Sichere Passwörter kann man sich selbst schwer ausdenken. Das ist auch gar nicht notwendig, denn KeePassXC erstellt für Sie Passwörter. Klicken Sie dafür in der Symbolleiste auf das „Würfel-Icon“.

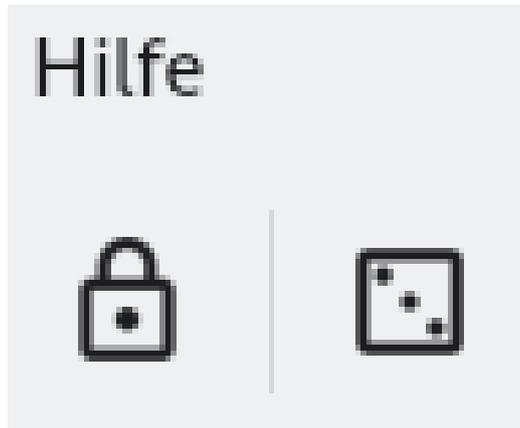


Abbildung 12: Der Würfel erstellt sichere Passwörter

In dieser Maske stellen Sie ein, wie Ihr Passwort aussehen soll.



Abbildung 13: Hier erstellen Sie Ihre Passwörter

5 Online Passwort-Manager Proton Pass

Proton Pass erhalten Sie hier. Protonpass gibt es auch als App für Mobilgeräte.

Laden Sie sich das für Sie passende Add-on herunter und installieren es. Wie man ein Add-on installiert, ist hier beschrieben.

5.1 Proton Pass in Betrieb nehmen

Um *Proton Pass* in Betrieb zu nehmen, klicken Sie auf das Symbol für Add-ons in Ihrem Browser, wie es hier beschrieben ist. Klicken Sie anschließend auf den Eintrag für *Proton Pass*. Es öffnet sich folgende Maske.

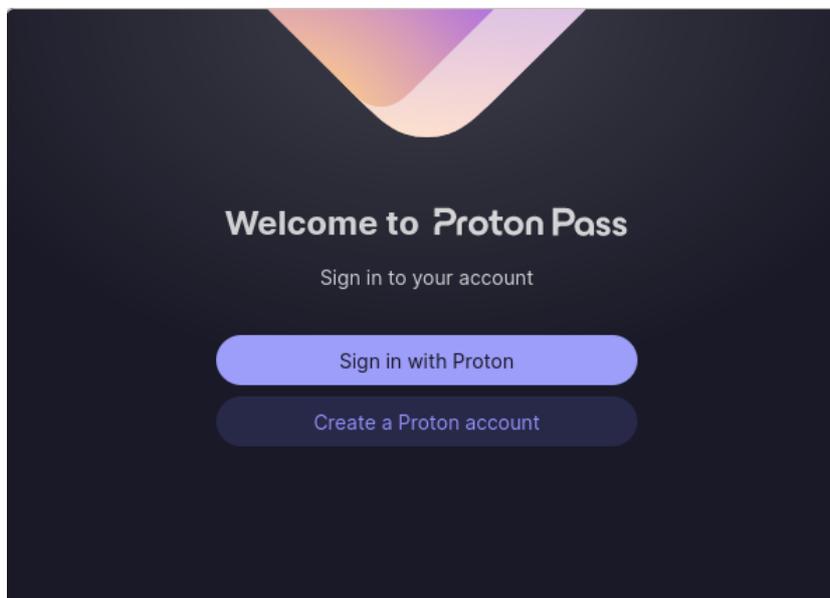


Abbildung 14: Klicken Sie auf *Create a Proton account*

Bestätigen Sie die neue Maske mit einem Klick auf **Erlauben**. Anschließend wählen Sie auf der **linken Seite** „**Proton free**“ aus.

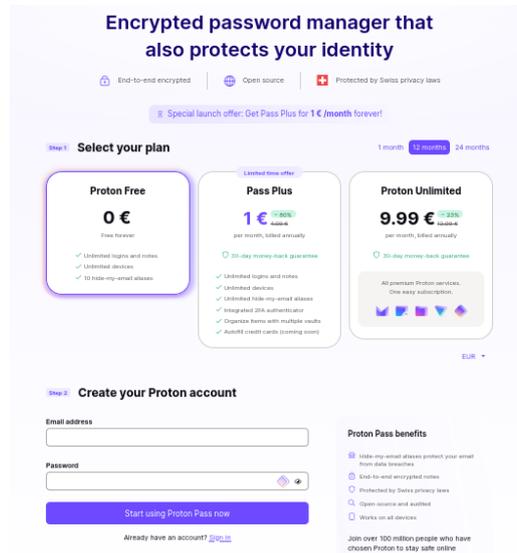


Abbildung 15: Erstellen Sie ein kostenloses Proton-Konto

Die Einrichtung ist selbst erklärend, daher gehe ich darauf hier nicht weiter ein.

Um sich bei **Proton Pass** anzumelden, gehen Sie auf die Option **Sign in**. Sie erreichen Sie entweder - bei einem Neustart Ihres Browsers - über einen Klick auf das **Add-on Symbol oben rechts** oder direkt nachdem Sie Ihren Account erstellt haben.

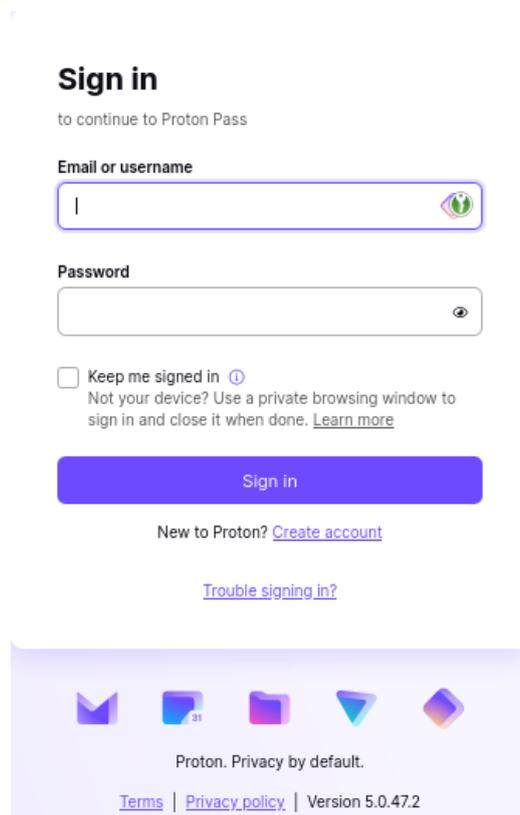


Abbildung 16: So sieht die Anmeldemaske aus

Nach dem ersten Einloggen kommen Sie auf eine Seite von Proton Pass, die Ihnen in einem Video den Umgang mit dem Online-Passwortmanager erklärt. Dieser Videoclip erklärt den Umgang so gut, dass es nicht sinnvoll wäre, die dortigen Erklärungen in dieses Skript aufzunehmen.

6 Quellen

1. KeePassXC (07.08.2023) - <https://keepassxc.org/>
2. KeePassXC-Browser für *Firefox* (07.08.2023) - <https://addons.mozilla.org/de/firefox/addon/keepassxc-browser/>
3. KeePassXC-Browser für *Chrome* (07.08.2023) - <https://chrome.google.com/webstore/detail/keepassxc-browser/oboonakemofpalcgghocfoadofidjkkk>
4. Proton Pass (07.08.2023) - <https://proton.me/de/pass>

Proton Pass - Getting started (07.08.2023) - <moz-extension://65a08ecf-1cf8-4238-994b-b66ac829f254/onboarding.html#/welcome>