Online Konten

Fast niemand kann heutzutage ohne Onlinekonten leben:
Stromanbieter, Stadtwerke, Telefon/Internetanbieter, Mobilfunkanbieter (Netz) bieten fast nur noch Rechnungen über Onlinekonten an und selbst wer die Rechnung analog per Brief bekommt (meist mit Aufschlag) hat trotzdem ein (ungenutztes) Onlinekonto.
Handys gibt es fast nur noch als Smartphone und sie lassen sich OHNE Konto weder einrichten noch benutzen.
99+% dieser Konten benötigen ein Email-Konto oder eine Telefonnummer (in der Regel Handynummer) um betrieben zu werden. Der früher mal genutzte Weg über wählbare Anmeldenamen ist quasi ausgestorben, denn ein Onlinekonto MUSS eindeutig sein, „Lieschen Müller" kann es selbst im selben Haus mehrfach geben.
Also alleine für ein benutzbares Smartphone benötigt man schon 2-4 Onlinekonten:

1. Ein E-Mailkonto unter dem das Handy (mit einer Emailadresse) angemeldet und betrieben werden kann, macht man das wie vom Betriebssystemanbieter vorgesehen existiert dieses dann im Konto unter 2. also kann man eins wegbekommen, dann ist aber auch beides in fremden Händen, wenn DAS Konto kompromittiert ist!
2. Das Konto beim Anbieter des Betriebssystem (in der Regel Apple mit IOS oder Google und fast alle anderen Telefonanbieter mit Android, chinesische Anbieter auch mit Android aber eigenen Konten, zusätzlich kann man z.B. bei Samsung noch ein eigenes Konto für deren Dienste nutzen, dann wären es schon 4 Konten die man hat  .
   Nur wenn man sich aus der recht nerdigen Nische der freien Smartphonebetriebssysteme bedient kommt man OHNE solch ein Konto aus.
3. Für Überblick, Administration des eigenen Telefontarifs und die Rechnungen noch ein Konto beim Telefonanbieter (T-Mobile, Vodafone, E-Plus, bzw. zig Reseller)

Jedes Onlinekonto benötigt eine Autorisierung (Authentifizierung), da sie ja im Internet abrufbar ist. In ganz seltenen Fällen, können Sie zumindest als Kunde erkannt werden, z.B. wenn Sie vom eigenen Telefonanschluss bei der Telekom anrufen, dito bei manchen Mobilfunkanbietern. Aber selbst dann wird man nach einer zusätzlichen Bestätigung gefragt, dass es auch wirklich Sie sind.

Am Telefon kann man das noch Menschen glaubhaft machen durch Abfragen irgendwelcher Daten. Eine Maschine verlässt sich auf Anmeldename (weltweit einzigartig!) und Passwort (bzw. neuerdings Passkey).

In Filmen wird oft gezeigt, dass man Passwörter erraten kann, besonders, wenn man etwas über das Gegenüber weiß. Ohne abzuschweifen, das ist in Zeiten Sozialer Medien noch leichter möglich. Deshalb sollen diese möglichst lang sein (es geht kaum noch unter 8 Stellen) und aus Groß- UND Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, Achtung bei Sonderzeichen, nicht immer sind dieselben bei unterschiedlichen Anbietern verwendbar, ein Leerzeichen geht manchmal, manchmal wird es abgewiesen und dummerweise wird es auch manchmal bei der Eingabe einfach unterdrückt. Man merkt so gar nicht, dass es NICHT Bestandteil des Passwortes geworden ist. Somit ist die eigene Kreativität und Speicherkapazität gefragt. Da Passwörter nicht unbedingt ständig gebraucht werden, vergibt ein Otto-Normalbenutzer in der Regel ein recht leicht Merkbares und nimmt dieses dann für alle/viele weitere Online-Konten.

Keine gute Idee, denn wenn ein Passwort einmal irgendwie bekannt geworden ist (Stichwort „Leak"), stehen mehrere Onlinekonten offen. Also könnte man auf die Idee kommen, Passwörter mit System zu vergeben (z.B. „Dienstkürzel mit Anfangsgroßbuchstaben, dasselbe Sonderzeichen, die gleiche Zahl wie Geburtsjahr/Hausnummer/etc."). Auch keine gute Idee, weil man das leicht erkennen und ausnutzen kann.

Also bleibt nur der Weg über Passwortlisten, die man auf Papier anfängt (Der Rechner könnte infiltriert werden und die Liste kopiert werden!) und die im Laufe von Jahren zu einer Krickelsammlung anwächst, „Hatte ich nun schon ein Konto für Ebay? Ach egal ich lege Eins an. Ach die Email ist schon in Verwendung? Egal, dann vergebe ich halt ein neues Passwort.“ Und schon hat man Duplikate in seiner Liste. Auch werden da oft irgendwelche bekannten Worte verwendet, weil man sich das ja „Schwiegermutter,123“ beim Eintippen leichter merken kann als „/+@Sh:4'“ obwohl das Erste wesentlich länger ist!

Solche eingängigen Worte können aber auch leichter mittels Passwortlisten geknackt werden als ganz zufällige Buchstabenlisten. Also ein Dilemma. Da hilft schon eine sogenannte 2 Faktor Authentifizierung (2FA oder auch manchmal MFA für MultiFaktorAuthentifizierung). Diese benötigt ein 2. Gerät, auf dem dann sichergestellt werden kann, dass es sich beim Anmelder um den Nutzer des Onlinekontos handelt. Als Beispiel: früher wurden bei Bankkonten mal sogenannte TAN-Listen verwendet die man in Papierform zugeschickt bekam.
Dann gibt/gab es 2FA per SMS, denn wenn das eigene Handy nicht in fremde Hände gelangt, kann man damit seine Identität bestätigen. Dummerweise hat man aber auch hier einen Weg gefunden diesen Schutz zu umgehen.

Also gab es sogenannte Einmalpasswörter (=TOTP „Time-based One-TimePassword“ = „Zeitbasiertes Einmalpasswort“) die auf einem Gerät erzeugt werden können. Der Vorteil ist, dass man diesen „Generator“ nicht einfach kopieren kann, außerdem ist seine Benutzung durch einen PIN/biometrisches Merkmal schützbar.

Aber auch diese Maßnahme lässt sich bei unaufmerksamen Nutzern ausnutzen, wenn man diese auf gleich aussehende Fakeseiten lenkt und ihnen dort quasi vorgaukelt sich beim eigenen Anbieter anzumelden und in Wirklichkeit meldet sich der Hacker stattdessen an und eh man sich versieht, hat er das Konto übernommen und man selbst ist ausgesperrt.

Man muss also genau aufpassen, WER einem eine Mail geschrieben hat (echte Adresse, nicht das was im Namen steht) und auf welcher Webseite(URL)/App man seine Zugangsdaten eingibt. Ungewöhnliche Verzögerungen beim Autorisieren, nicht identische Transaktionscodes (den man z.B. bei manchen Banken auf die App mit übermittelt bekommt, sind ALARMZEICHEN!)

Gegen diesen menschlichen Fehler helfen dann Passkeys, mit dazukommenden Einschränkungen (Entweder an eine Hardware gebunden, die kaputtgehen kann oder die Passkeys werden über Cloudanbieter gesichert und synchronisiert, d.h. man muss dem Cloudanbieter vertrauen.

Daher als ersten Schritt Passwortverwaltung in selbst verwaltete, rechnerunterstützte Hände legen. Ein Passwortmanager muss her.

Passwortmanager gibt es viele, am sinnvollsten nimmt man einen der auch digitale Souveränität bietet und gut verbreitet ist, damit man ihn sicher und langlebig nutzen kann. Bitwarden und Keepass sind solche Vertreter (Open Source) und beide unterstützen inzwischen sowohl TOTP; als auch Passkey. Die Daten mit denen der TOTP oder Passkey berechnet wird sind mittels des Tresorpasswortes geschützt, können aber einfacher verteilt und gesichert werden. Apps auf Handy/Windows nutzen nicht-auslesbare Sicherheitschips in denen diese Schlüssel verwahrt werden, ebenso wie Hardwareschlüssel die man per USB oder/und Bluetooth oder NFC nutzen kann (auch nur per Biometrie oder Passwort freigebbar). Hier sind die Schlüssel an das Gerät gebunden und bei Verlust/Defekt sind die TOTP & Passkey weg.

Bei Bitwarden kann man sich sogar eine Plattform für die Onlinesynchronisation monatlich mieten (1,65€/Monat), dann erübrigt sich ein eigener Onlinespeicher, etc. und mögliche Angriffe auf die ansonsten verschlüsselte Tresordatei, bei Bitwarden steht ja keine Organisation dahinter, die Interesse haben könnte, an Ihre Passworte zu gelangen, so dass man da recht sicher sein kann. Keepass setzt auf Eigenverantwortung der Nutzer, auf den nächsten Seiten eine Kurzanleitung Keepass einzurichten und zu nutzen.

Keepass (Bzv. neuere Variante KeepassXC) einrichten

- Download über die Seite https://keepassxc.org/download/ (dort für Windows/Mac/Linux, Android im Google PlayStore oder im Alternativen, freien AppStore Fdroid). Unter Linux gibt es auch eine Flatpack Version, die kann aber bei dem komfortablen Zusammenspiel mit Browserplugins zum automatischen Einfügen Problem bereiten.
- Installieren, dabei wird man nach dem Namen des Tresors und einem Passwort für den Tresor gefragt, Da sich dahinter demnächst ALLE Online-Konten verbergen empfiehlt sich ein recht kompliziertes Passwort. Um sich das besser merken zu können (Keine Sorge, man muss es öfters eingeben und dadurch merkt man es sich dann im Laufe der Zeit) wäre eine gute Idee, einen bekannten längeren Satz zu nehmen, z.B. der Anfang des Gedichtes „Herr von Ribeck zu Ribeck im Havelland, ein Birnbaum in seinem Garten stand“. Nun nimmt man die Anfangsbuchstaben und Punktionen, also „HvRzRiH,eBisGs.“, nun „ersetzt“ man noch ein paar Buchstaben durch Zahlen „HvRzR1H,3B15G5.“ (Das nennt sich „Leetspeak“, siehe Leetspeak - Wikipedia) und schon hat man ein nicht leicht erratbares Passwort mit allem was man braucht. Es verschlüsselt den Passworttresor, in dem sich demnächst viele Passwörter, TOTPs und Passkeys befinden und das man leicht speichern und sogar über Onlinekonten auf verschiedene Geräte synchronisieren kann.
- Noch liegt der Ort auf dem PC. Man kann aber auch einen Ordner eines Onlinespeichers wählen, die man am PC angebunden hat (und auch am Handy).
  Wem das zu viel Aufwand ist, der kann eine Kopie auf einem USB-Stick mit der aktuellen Version mitnehmen, in der Regel ändert man ja nicht ständig Passworte oder fügt neue Onlinekonten hinzu, dann reicht in der Regel auch eine etwas ältere Version. Selbst mit hunderten Onlinekonten bleibt die Datei unter einem Megabyte!!!
- Die Standardeinstellungen kann man erstmal so lassen und sich später schlaumachen, was man daran ändern kann. Nutzt man ein und dieselbe Datei von mehreren Rechnern gleichzeitig auf einem Onlinespeicher, sollte man im Menü unter „Werkzeuge“, „Einstellungen“, „Keeshare“, „Import„ und „Export“ aktivieren und einen Namen als „Unterzeichner“ angeben.
- Ebenso sollte man nachschauen, ob links unter „Allgemein“ in der Rubrik Datenverwaltung alle Haken außer dem Letzten gesetzt sind (den braucht man nur bei Problemen während Speicherung auf Onlinekonten). Somit werden alte Tresore gesichert und möglichst schnell geschrieben und gelesen.
- Man kann nun Einträge in Ordnern strukturiert anlegen, diese mit Zusatzinformationen und Icons versehen, TOTPs und Passkeys dazupacken, ausserdem gibt es einen Papierkorb und Zeitstempel von Anlage-/Änderungsdatum und für Passworte, die mal ablaufen.
- Videotutorials gibt es auch wie Sand am Meer, Hilfstellungen kann auch Google bieten, wobei man immer schauen muss, denn die Community entwickelt die Programme flott weiter und manchmal sucht man etwas an einer inzwischen veralteten Stelle. Da hilft mehrfach suchen, oder die Angabe der Versionsnummer oder im schlimmsten Fall bei der Community nachfragen. Antworten bekommt man eigentlich immer recht schnell.

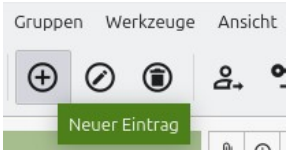
Hier die Linkliste aus der Präsentation:

Die häufigsten Passworte 2025	Hasso Plattner Institut
Passwortwechsel war gestern	Bundesamt für Sicherheit in der Informationstechnologie
Jahresplan zur digitalen Souveränität	gnu0os0ta (ein österreichischer „Open Source Aktivist“)

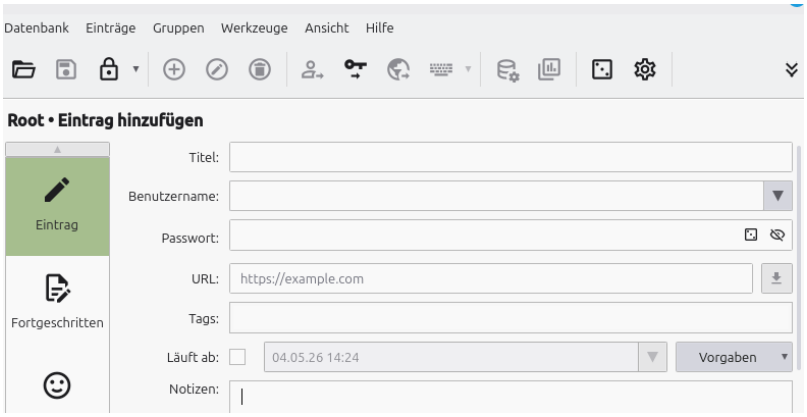
Seine Vorlage zur Bestandsaufnahme (überarbeitet)

Auf den folgenden Seite ein Kurzabriss zur Erstellung eines neuen Passworts in Keepass.

1. Einen neuen Eintrag über das Menü (Pluszeichen im Kreis) anlegen:

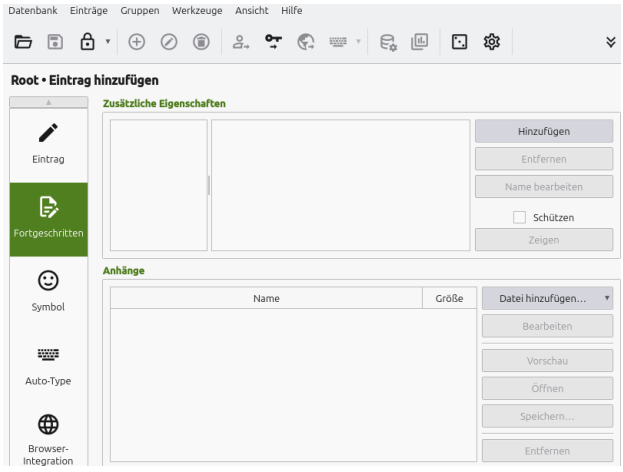


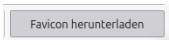
2. Das Formular ausfüllen:



Als „Titel“ vergibt man einen sprechenden Namen. Als „Benutzername“ den Anmeldenamen. Um ein schweres und langes Passwort zu generieren kann man oben das Würfelzeichen nutzen. Bei der „URL“ ist WICHTIG, das Protokoll zu beachten, inzwischen fast immer „HTTP**S**://“ (das unverschlüsselte „HTTP://“ kommt fast kaum noch zum Einsatz). Mit „Tags“ (=Aufkleber) kann man Passworte auch in verschiedenen Ordnern nochmals gruppieren, weil man danach suchen kann.

3. Auf der linken Seite unter „Fortgeschritten“ kann man Oben zusätzliche Felder, die auch geschützt werden können (dort stehen auch TOTP und Passkey Schlüssel) und Unten Dateianhänge anfügen.



4. Unter Symbol kann man ein Icon auswählen. Oft bringen Webseiten selbst ein Icon mit, welches man mit dem Button 

herunterladen kann. Fortgeschrittene können auch selbst ein Icon erstellen/irgendwoher laden und das dann einbinden.

5. Am Ende mit OK abspeichern; man kann Einträge mittels Maus Drag’n’Drop in (selbst angelegte) Ordner verschieben.