COMPUTERIA SOLOTHURN

Merkblatt «Passwort-Verwaltung»

Immer diese Passwörter!

Immer wieder müssen auf denselben Webseiten die gleichen Benutzernamen und Passworte eingegeben werden, z.B. für die Anmeldung beim Webmail:

Das nervt! Wer keine allzu hohen Sicherheitsanforderungen stellt, kann die in Windows 10 und macOS eingebauten – und somit kostenlosen – Passwort-Verwaltungen benützen.

Passwort-Verwaltung in Edge unter Windows 10

Mit Edge/Windows 10 muss die Passwort-Verwaltung erst aktiviert werden, bevor sie zur Verfügung steht. Dazu in Edge ganz rechts oben das …-Menü öffnen und dort zuunterst die «Einstellungen». Im Einstellungsfenster den Punkt «Kennwörter & AutoAusfüllen» wählen und die erste Option aktivieren. Mit den übrigen könnten auch Formular- und Kreditkartendaten zum automatischen Einsetzen gesichert werden. – Dort findet sich auch der Link zum Verwalten für die gespeicherten Kennwörter, wobei allerdings nur recht rudimentäre Möglichkeiten geboten werden. Zum Verwalten muss jedes Mal auf die gleiche umständliche Art zu diesem Link navigiert werden.

Wo immer online-Dienste benützt werden, wird eine Anmeldung verlangt. Im einfachsten Fall – z.B. für Webmail-Dienste des Internet Service Providers wie im Bild oben – liegen Benutzername und Passwort vor und können im Anmeldeformular eingegeben werden.

Nach Auslösung der Übermittlung der gemachten Angaben wird die Frage, ob das Kennwort gespeichert werden soll, ganz zuunterst im Edge-Fenster angezeigt, leider etwas ausserhalb des Blickfeldes:

In den meisten Fällen erfordert die erstmalige Benützung eines online-Dienstes eine Registrierung. Je nach Dienst sind die Registrierungsprozeduren ziemlich verschieden. Als Beispiel hier das Registrierungsformular für die Seite von SRF. Eine Registrierung bei SRF benötigt, wer Artikel auf deren News-Seite kommentieren möchte. Leider gibt Edge weder beim Eingeben der persönlichen Daten noch bei der Definition eines sicheren Passwortes irgendwelche Unterstützung.

Nach dem Klick auf ACCOUNT ERSTELLEN wird ebenfalls gefragt, ob die Angaben gesichert und beim nächsten Login automatisch eingesetzt werden sollen.

Wird später eine Seite aufgerufen, für welche das Passwort gesichert wurde, so wird dieses automatisch eingesetzt, so dass die Übermittlung nur noch ausgelöst werden muss. Sind für eine Seite mehrere Anmeldekombinationen gespeichert worden, so werden diese zur Auswahl angeboten:

Trotz aller Kritik: Um das ewige Eingeben von immer gleichen Anmeldekombinationen zu vermeiden, ist auch diese rudimentäre Passwortverwaltung durchaus geeignet.

Passwort-Verwaltung in Safari unter macOS

Nach der Systeminstallation ist die Passwort-Verwaltung in macOS automatisch aktiv. Werden zum ersten Mal auf einer Login-Seite Benutzername und Passwort eingegeben und deren Übertragung ausgelöst, so fragt das System, ob das Passwort gesichert werden soll:

Beim nächsten Aufruf der Seite wird die gespeicherte Benutzernamen-/Passwortkombination angeboten und nach Klick eingesetzt. Sind mehrere Anmeldekombinationen für die aufgerufene Seite gesichert, stehen diese wie bei Edge zur Wahl:

Im Gegensatz zu Edge ist Safari bei der Registrierung für einen onlie-Dienst behilflich: wird im ersten Eingabefeld auf das Personensymbol rechts geklickt, füllt Safari alle Angaben ein, die für die Identität von früheren Eingaben her bekannt sind.

Werden an und für sich bekannte Angaben nicht ausgefüllt, so ist dies nicht der Fehler von Safari, sondern der nicht normgerechten Codierung der Seite. Die Passwort-Verwaltung von macOS ist aber auch behilflich, um ein geeignetes Passwort zu definieren. Ein Klick auf das Schlüsselsymbol rechts genügt …

… und ein sicheres Passwort wird nicht nur ins Eingabefeld, sondern auch gleich ins Feld eingetragen, in welchem das gleiche Passwort zur Sicherheit wiederholt werden muss.

Für die Verwaltung der gespeicherten Passwörter wird das Dienstprogramm «Schlüsselbundverwaltung» benützt, mit dem Passwörter gelöscht oder kopiert werden können, wobei für sicherheitsrelevante Operationen die Eingabe des Hauptpasswortes erforderlich ist.

Auf weitere Möglichkeiten der Mac-Schlüsselbundverwaltung wird hier nicht eingegangen. Insbesondere wer sich für die Synchronisation der Passwörter zwischen Mac und iOS-Geräten (iPad, iPhone) interessiert, findet ein gute Anleitung unter diesem Link: https://support.apple.com/de-ch/HT204085

Spezielle Passwort-Verwaltungsprogramme

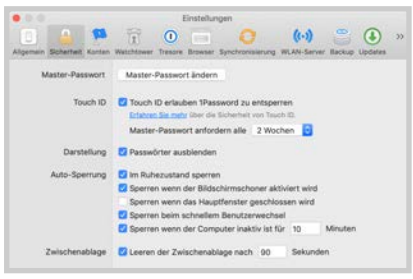
Wer höhere Sicherheitsansprüche stellt oder wem die Möglichkeiten der systemeigenen Programme sonst nicht genügen – angesichts der etwas rudimentären Funktionen wohl insbesondere Windows-Benützer – installiert ein eigentliches Passwort-Verwaltungsprogramm. Es gibt unzählige solche Programme, viele auch – mindestens vermeintlich – kostenlos. Aber aufgepasst: häufig gibt es zur kostenlosen Version eine kostenpflichtige Parallelversion, ohne die wichtige Funktionen nicht zur Verfügung stehen. Die Kosten können dabei ganz ordentlich ins Gewicht fallen, wenn z.B. die Anzahl Passworte bei der Gratisversion beschränkt ist, oder die Synchronisation mit dem Smartphone die Kostenpflicht auslöst, im ungünstigen Fall sogar mit einem Miettarif. Es lohnt sich also, sich genau zu informieren, bevor der Entscheid für ein bestimmtes Programm getroffen wird.

Wirklich gute Passwort-Verwaltungsprogramme bieten alle ähnliche Funktionen, mindestens vergleichbar mit dem Verwaltungsprogramm von macOS.

Bevor ein solches Programm benützt wird, sollte die systemeigene Passwortverwaltung ausgeschaltet werden. Sonst kommt es zu Verwirrungen. Mit macOS müssen dazu in den Einstellungen von Safari unter «Autom. ausfüllen» alle Optionen deaktiviert werden.

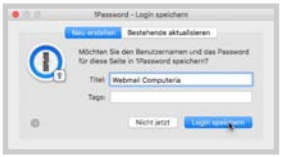
Als Beispiel für spezialisierte Passwort-Verwaltungsprogramme werden hier ein paar zusätzliche Funktionen des von mir seit Jahren benützen Programms «1Password» gezeigt.

Alle Funktionen des Programms müssen immer wieder durch Eingabe eines Hauptpasswortes oder Identifikation mit Touch ID oder Face ID freigeschaltet werden. In den Einstellungen stehen in der Rubrik «Sicherheit» sehr viele Möglichkeiten zur Verfügung um zu bestimmen, unter welchen Umständen die Freigabe verfällt:

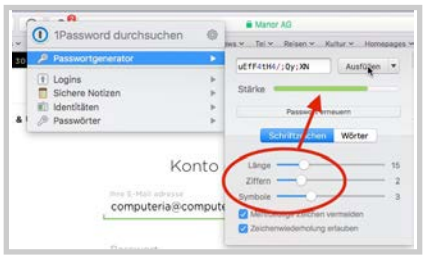


Welche Optionen gewählt werden sollen, hängt davon ab, wer alles wie leicht Zugang zum Computer hat.

Die Speicherung von Anmeldekombinationen und deren Benützung sind ähnlich wie mit den systemeigenen Verwaltungen. Jeder solchen Kombination kann ein eigener Name zugeteilt werden, was deren Identifikation beim Verwalten erleichtert:



Wird beim Anmelden zu einem online-Dienst ein Passwort vorgeschlagen, so lassen sich dessen Eigenschaften beeinflussen:



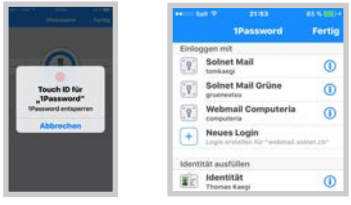
So kann ggf. Forderungen des Dienstes nach bestimmten Eigenschaften des Passwortes Rechnung getragen werden. Die sich ergebende Stärke des Passwortes wird angezeigt.

Wichtig bei solchen Programmen ist auch, dass sie für alle in Betracht kommenden Plattformen in kompatibler Form zur Verfügung stehen und die automatische Synchronisation zwischen mehreren Computern, Tablets und Smartphones erlauben.

Auf einem iPhone sind die Passworte ganz einfach zu benützen. Zwar muss gelegentlich auch das Hauptpasswort eingegeben werden, so insbesondere nach jedem vollständigen Ausschalten des Gerätes. Normalerweise genügt aber die Erkennung des Fingercodes (Touch ID). Hier der typische Ablauf:

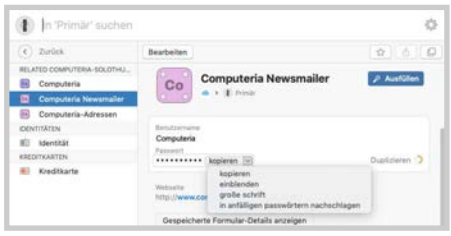
Nach Antippen des Teilen-Symbols kann 1Password aufgerufen werden.

Es folgt die Aufforderung zum Finger-Auflegen, …

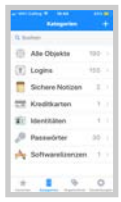


… wonach die für diese Webseite gespeicherten Anmeldemöglichkeiten zur Auswahl angeboten werden.

Die Details eines Passwortes können auf allen Plattformen aufgerufen werden. So kann z.B. eine Anmeldekombination für eine neue Webseite des gleichen Dienstleisters einfach übernommen werden.



1Password kann neben Passworten und Identität noch andere Informationen speichern:



Unter «Sichere Notizen» hat z.B. mein Sohn die Zugangsdaten zu meinem Computer und das Hauptpasswort meines 1Password abgelegt und kann so im Notfall ohne Probleme auf alle wichtigen Daten in meinem Computer zugreifen.

Sicherheit sollte etwas Wert sein! Bei professioneller Software ist die Gewähr am grössten, dass sie langfristig gepflegt und neuen Betriebssystem-Versionen rasch angepasst wird. Die Verfügbarkeit der gewünschten Funktionen ist aber beim Entscheid für ein Programm Voraussetzung! «1Password» gibt es, wie diverse andere professionelle Programme, für die gängigen Plattformen Windows, macOS, Android und iOS. Die Synchronisation zwischen den Geräten erfolgt automatisch über eine Cloud.

Eine Kaufversion von 1 Password wird auf der Seite https://1password.com/de/downloads/ angeboten. Mit der Abo-Version (https://1password.com/de/sign-up/) kann bei Verlust des eigenen Gerätes von einem fremden Computer unter den nötigen Sicherheitsvorkehrungen auf die Passworte zugegriffen werden.

Alternative für Windows

Co-Referent Martin Dürig setzt für Windows mit Erfolg ein völlig kostenloses Open-Source-Programm ein: KeePass. Mehr dazu auf dieser Webseite: http://keepass.info/index.html

Mac-, iOS- und Android-Versionen gibt es auch von diesem Programm. Aber sie sind nicht in gleich komfortabler Art plattformübergreifend zu verwenden wie professionelle Programme.