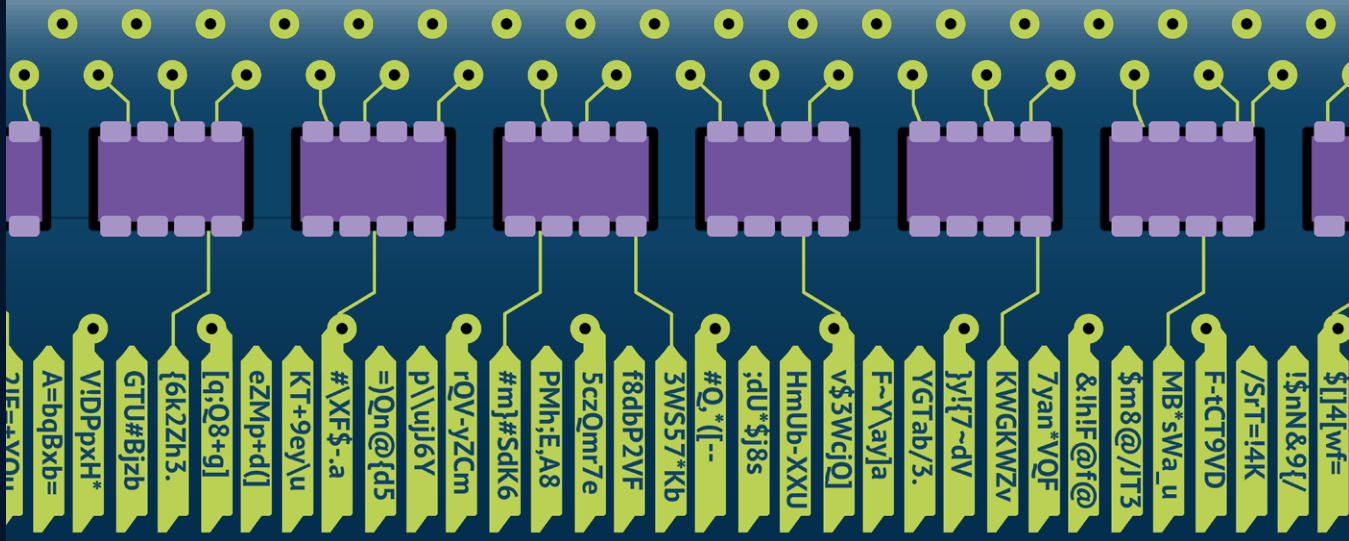
Passwortverwaltung:

Den Überblick über Kennwörter behalten



Online unterwegs zu sein, bedeutet auch, sich bei diversen **Portalen und Plattformen** mit **Benutzernamen und Passwort** anzumelden. Sei es beim **E-Mail-Konto**, den **Sozialen Medien** oder beim **Onlineshopping** – ohne Passwort geht es nicht. Und bei all diesen Diensten sollte, wenn möglich, auch **nicht immer das gleiche Kennwort** verwendet werden. Doch wie sich die vielen verschiedenen Kombinationen merken?

Eine übersichtliche **Passwortverwaltung** kann das Leben da um einiges erleichtern. Über verschiedene Varianten sind Nutzer in der Lage, ihre **Passwörter zu verwalten**, was zudem auch den **Überblick** über bestehende und verwendet Kennwörter vereinfacht. Allerdings sollte die Sicherheit bei allen Versionen einer solchen **Passwortverwaltung** immer im Mittelpunkt stehen.

Wie Internutzer **Passwörter sicher verwalten**, welche **Vor- und Nachteile** die verschiedenen Formen der **Passwortverwaltung** haben und was besonders zu beachten ist, betrachtet dieser Ratgeber näher.

Inhalt

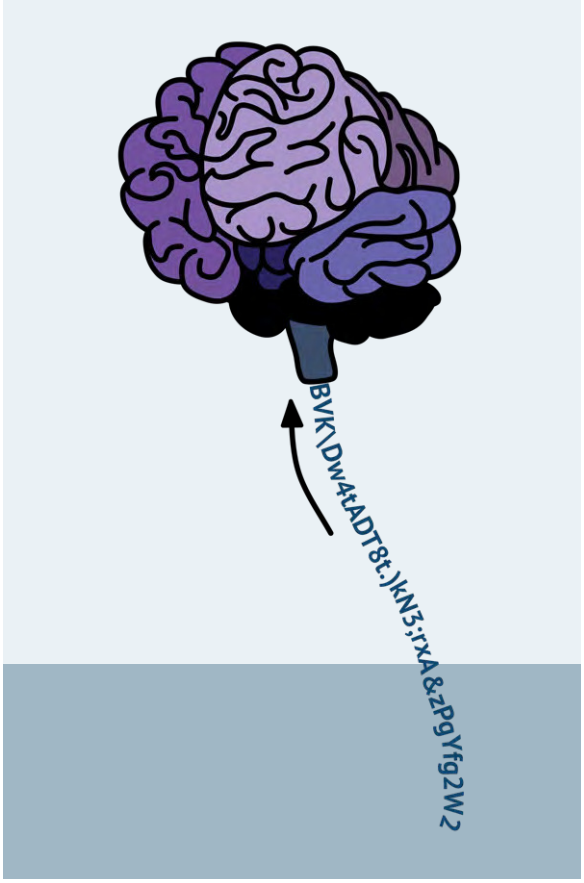
Worum handelt es sich bei einer Passwort-verwaltung?

Einige Menschen können sich die umfangreichsten **Kombinationen aus Zahlen, Buchstaben und Sonderzeichen** leicht merken und müssen ihre **Passwörter** nirgendwo aufschreiben oder hinterlegen. Allerdings bilden sie wohl eher die Ausnahme. Um sich an die Zugangsdaten zu den verschiedensten **Onlinediensten** erinnern zu können, speichern viele diese einfach in ihrem **Browser** oder der jeweiligen **App**.

Das macht diese aber auch **anfällig** dafür, **gehackt** und **gestohlen** zu werden. Da stellt sich dann oft die Frage, ob eine **organisierte zentrale Passwortverwaltung** sicherer ist und Anwender dennoch schnell auf ihre **Onlinekonten** zugreifen können. In der Regel handelt es sich dabei um eine **Form des Speicherns von Passwörtern**, welches es ermöglicht, sich bei Webseiten, Portalen und Netzwerken anzumelden, **ohne Gefahr** zu laufen, bei zu häufigen **Falscheingaben** gesperrt zu werden.

Egal ob online oder offline, als Software, App oder Portal, das Prinzip für eine sichere Passwortverwaltung ist bei allen vorhanden Varianten ähnlich. Die Zugangsdaten werden gebündelt hinterlegt und üblicherweise dort gespeichert, wo nur der Besitzer Zugang hat.

Bei den modernen Versionen bedeutet dies, dass die gesamten **Benutzerdaten verschlüsselt gespeichert** werden. Um an diese



Daten zu gelangen, ist in der Regel dann ein einziges sogenanntes **General-, Haupt- oder auch Masterpasswort** notwendig. Dieses eine **Passwort** können sich die meisten entweder merken oder durch eine **Eselsbrücke** in Erinnerung rufen.

Das heißt, nur derjenige, der das **Masterpasswort** besitzt, kann auf die hinterlegten **Daten** zugreifen. Einige Programme und Apps besitzen Funktionen, die **sichere Passwörter generieren** und dann auch verwalten können.

Verschiedene Arten Passwörter zu verwalten

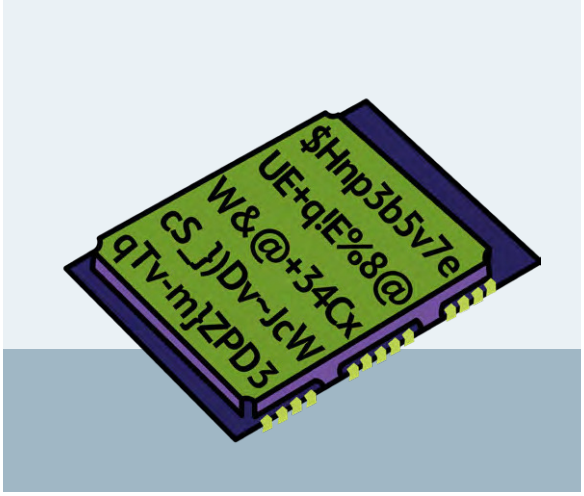
Kennwörter zu verwalten, kann auf die verschiedensten Arten geschehen. Sowohl **offline** als auch **online** können Nutzer ihre **Passwörter speichern und verwalten**. Ob aufschreiben, digital hinterlegen oder sie Programmen anvertrauen, ist dabei ihnen selbst überlassen.
In der Regel wird heute eher die technische Variante, die auf **Software** oder **Online-plattformen** zurückgreift und die Daten verschlüsselt, als **Passwortverwaltung** bezeichnet. Eine solche **Verwaltung** kann jedoch auch, wie zuvor erwähnt, mit Hilfe von Programmen, Apps oder Plattformen erfolgen.

Grundsätzlich gilt immer, dass Passwörter nur so sicher sind wie ihr Aufbewahrungsort.

Passwort durch Verwaltungsprogramm oder App sicher hinterlegen

Ein Passwort durch ein **Verwaltungstool** auf dem PC oder als App auf dem mobilen Gerät sicher zu verwalten, kann ein sinnvoller Gedanke sein. Besonders dann, wenn **viele Passwörter** vorhanden sind, die alle sicher sein sollen und dadurch auch schwer zu merken sind.

Ein Programm zur **Passwortverwaltung** hinterlegt die **Daten verschlüsselt** in einer Datenbank auf der Festplatte des Computers respektive auf dem Gerätespeicher, wenn



eine App verwendet wird. Einige bieten zudem auch eine Ablage **online in einer Cloud**, sodass die **Zugangsdaten doppelt gespeichert** sind. Auch bei einer **Passwort-verwaltung** durch eine App kann bei einigen Anbietern eine **Synchronisierung mit einer Cloud** eingerichtet werden.

Nach der Eingabe eines **Masterpassworts** gibt die Software die **Daten** frei, sodass diese von den jeweiligen Webseiten herangezogen werden können. Auch ist es möglich, die Daten nach **Kategorien** zu ordnen, was den Zugriff sowie den **Überblick** über die abgelegten Benutzerkonten zusätzlich erleichtert.

Gut funktionierende Apps oder Software für die Passwortverwaltung sind auch kostenlos erhältlich. Möchten Nutzer zusätzliche Funktionen haben, sind diese in den Programmen oder Apps meist kostenpflichtig.

Passwortverwaltung online

Passwörter im Browser zu speichern, kann verlockend sein, da ein schneller Zugriff auf die Daten möglich ist und keine weiteren Programme oder Erweiterungen installiert werden müssen. Einige bieten sogar die Option, Zugangsdaten per **Masterpasswort** zu schützen und so einen Zugriff nur für den Inhaber dieses **Passwortes** zu erlauben. Allerdings besteht hier oft die **Gefahr**, dass die im Browser aufbewahrten **Daten von anderen ausgelesen** werden können.

Daher ist für viele diese Art der **Passwortverwaltung** ungeeignet. Besonders Unternehmen setzen bei **sensiblen Daten** dann doch auf **professionelle Modelle**, um ihre **Passwörter** off- bzw. online zu verwalten.

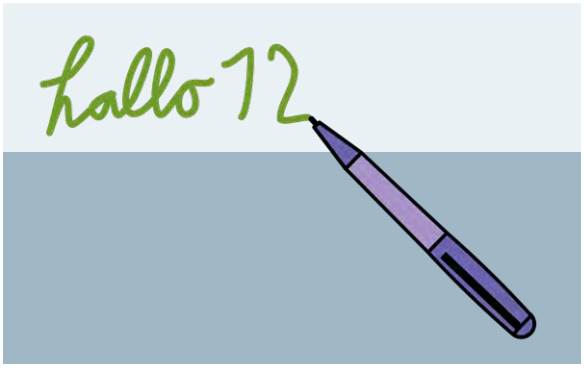
Neben der Variante, die Passwörter im Browser zu hinterlegen, können diese auch online bei verschiedenen Plattformen, die ähnlich wie die Verwaltungsprogramme funktionieren, gespeichert werden. Solch ein Passwortsafe kann Passwörter allerdings nur online verwalten und speichern. Das heißt, der Rechner muss mit dem Internet verbunden sein, damit Zugriff auf die Daten besteht. Falls Nutzer die Daten offline benötigen, kann das mitunter zu Problemen führen. Diese Plattformen können jedoch auf beliebig vielen Rechnern angewendet werden und benötigen keine Software oder Speichermedien.

Die online verfügbaren **Plattformen zur Passwortverwaltung** nutzen in der Regel eine **Erweiterung**, die im Browser installiert wird und so die hinterlegten Daten abrufen kann.

Passwörter offline verwalten

Viele Nutzer kennen auch andere Formen als eine Art **Passwortverwaltung**. Ganz klassisch wird ein **Buch oder Heft** angelegt, in dem die **Passwörter** aufgeschrieben sind. Das gleiche Prinzip verfolgt auch das Anlegen von Dokumenten auf dem eigenen Rechner. Die **Zugangsdaten** müssen hierbei jedoch jedes Mal neu bei den entsprechenden Diensten eingegeben werden. Diese Art der **Kennwortverwaltung** ist jedoch **nicht zu empfehlen**. Die **Daten im Dokument** können **bei Angriffen leicht im Klartext ausgelesen werden**. Auch ist es möglich, dass **Dritte** sich auf dem Rechner **Zugang zum Dokument** verschaffen und die **Daten missbrauchen**. Darüber hinaus können **alle Informationen** verloren, wenn das Dokument **aus Versehen gelöscht** wird, **beschädigt** ist oder das **System abstürzt**.

Ein **Verwaltungsprogramm** oder Passwort-Tresor bieten in der Regel die Chance, die Daten lokal auf dem Rechner oder einem Speichermedium sicher zu **verschlüsseln**. Auf die **Passwörter** kann auch dann zugegriffen werden, wenn der Rechner **offline** ist Nutzer aber Daten anpassen oder löschen möchten.

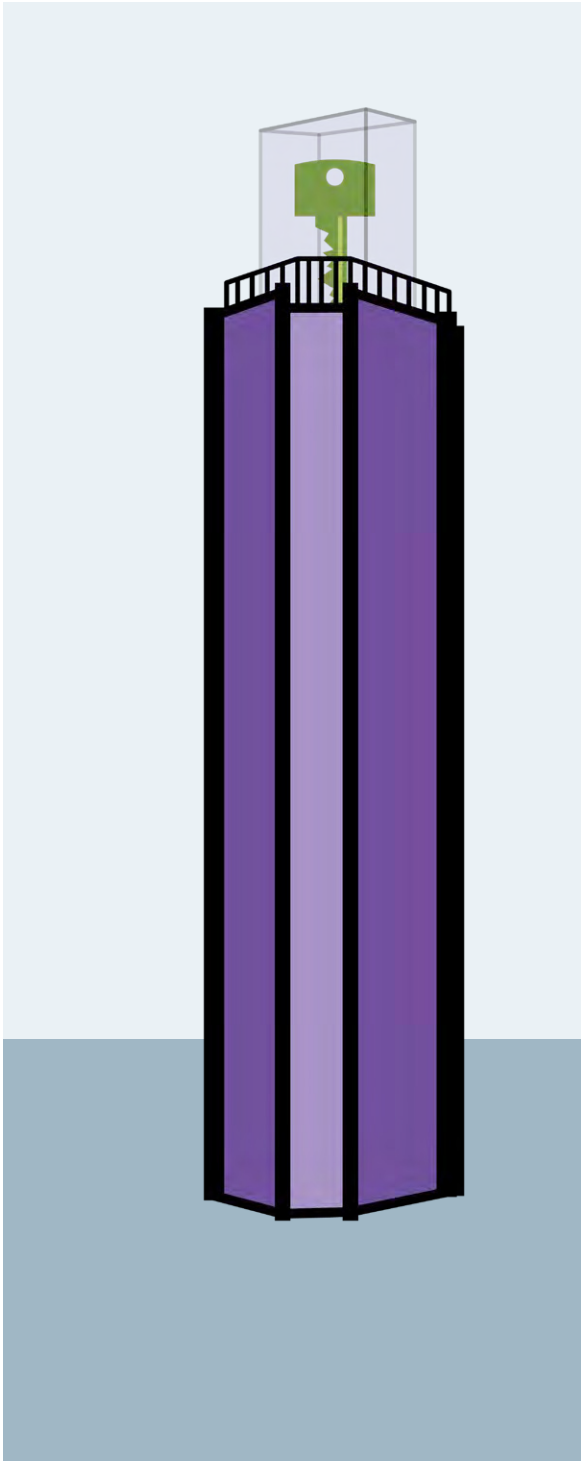


Warum ist die richtige Passwortverwaltung wichtig?

Bevor sich Anwender für eine Version der **Passwortverwaltung** entscheiden, sollten sie sich über die verschiedenen **Programme, Apps** und **Portale** genau informieren. Die **Vor- und Nachteile** jeder Version sollten dann den Ausschlag geben, welche für die **Bedürfnisse** und auch für das **Sicherheitsgefühl** des Nutzers die richtige ist.

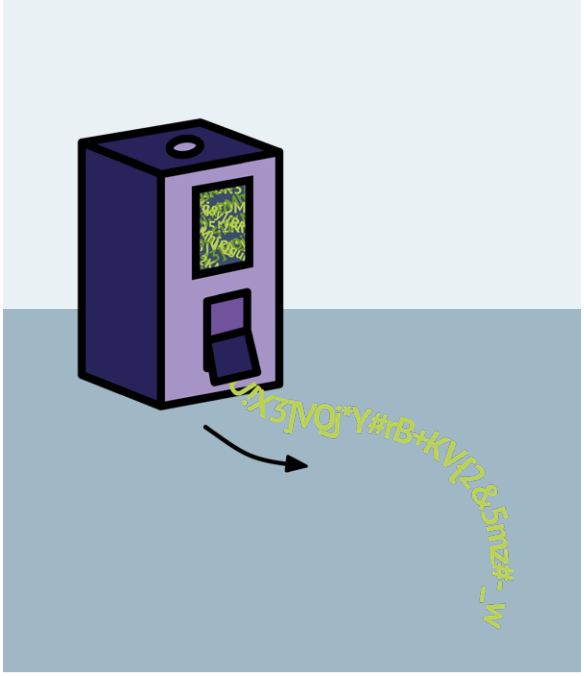
Sind die **Passwörter verschlüsselt** und so hinterlegt, dass nur bestimmte Personen Zugang haben, verringert sich das **Risiko**, dass die Daten einem Missbrauch zum Opfer fallen. Eine gute **Passwortverwaltung** kann also durchaus zur **Sicherheit** beim Umgang mit Daten und dem Surfen im Internet beitragen.

Zudem bieten die Programme, wie erwähnt, oft auch die Funktion, **sichere Passwörter zu generieren**, was bei einem generellen **Masterpasswort** durchaus sinnvoll ist. Ein sicheres Passwort zu erstellen, welches **Buchstaben, Zahlen** und **Sonderzeichen** enthält, ist in der Regel bei jedem Onlinedienst **zu empfehlen**. Diese lassen sich erfahrungsgemäß weniger häufig knacken. Sind diese dann auch sicher durch eine **Passwortverwaltung** hinterlegt, haben Nutzer eigentlich ihr Möglichstes getan, um einen Angriff auf ihre Daten zu unterbinden.



Pro und Kontra der Passwortverwaltung

Wie alle Anwendungen hat auch eine **Passwortverwaltung** ihre **Vor- und Nachteile**. Für welche Variante und ob sich ein Nutzer für eine **Passwortverwaltung** entscheidet, bleibt ihm überlassen.



VORTEILE

- **Alle Passwörter verschlüsselt** in einer **Datenbank** hinterlegt
- **Zugangsdaten** über einen **Online-Tresor**
- Es muss nur ein **Masterpasswort** angelegt werden
- **Zugang durch Fremde** wird durch die **Verschlüsselung** unterbunden
- Oftmals können Programme bzw. Portale zur Passwortverwaltung **sichere Passwörter generieren**, was den Zugang zu den Onlinediensten **sicherer** gestaltet

NACHTEILE

- Nutzer sind **abhängig** von einer einzigen Datenbank; **Sicherungskopien** sollten immer erstellt werden
- Die Daten sind bei einem **Online-Tresor nur online** verfügbar, was **offline** zu **Problemen** führen kann, wenn die **Passwörter** nicht noch woanders hinterlegt sind
- Geht das **Masterpasswort** verloren, sollte die verwendete Version über eine **Wiederherstellungsfunktion** verfügen, ansonsten könnten alle gespeicherten Daten unzugänglich werden
- Bei einen **Angriff, Hack oder Diebstah**l sind sofort alle Daten in falschen Händen
- Sind Programm/App/Portal **fehlerhaft**, können hierdurch **generierte Passwörter** nicht mehr nachvollzogen werden, was einen Zugriff auf Dienste erschweren kann

Impressum

Unter diesem Link gelangen Sie zu unserem Impressum: **Impressum**