# DIE BESTEN KOSTENLOSEN PASSWORT-MANAGER

**Passwort-Manager sind praktisch und sicher. Mit diesen kostenlosen Passwort-Managern sichern Sie Ihre Passwörter und vergessen Sie garantiert nie wieder.**

**KeePass**

Eine populäre Lösung für die Passwortverwaltung ist **KeePass.** Das Tool ist quelloffen, sodass Experten dessen Quellcode sichten können (Audit). So ist sichergestellt, dass es keine Hintertüren gibt. Der Open-Source-Gedanke hilft, Sicherheitslücken zu schließen: Sollte jemand einen Bug finden, kommt vermutlich alsbald ein Update, das ihn beseitigt. Die Oberfläche von KeePass ist angestaubt, die Bedienung ist binnen einiger Minuten Einarbeitung zu erlernen.

Der größte Vorteil ist auch ein Nachteil: Die Speicherung Ihrer Logins erfolgt lokal, daher wandern sie nicht auf fremde Server, wo sie Hackern ausgesetzt sein könnten.

Jedoch müssen Sie sich selbst um Virenschutz, Backups und eine Synchronisation Ihrer Logins aufs Smartphone kümmern. Den Funktionsumfang erweitern Sie mit jeder Menge Plug-ins. Das ist reizvoll, aber ein theoretischer Sicherheitsnachteil: Im Einzelfall sind die Zusatztools eventuell unsicher. KeePass ist zu Recht eines der bekanntesten Passworttools – auch diese Lösung kommt mit einem Passwort-Generator daher.

Hersteller von Antivirenprogrammen bieten Passwort-Manager häufig als Zusatzfunktion an. So gibt es beispielsweise Passwort-Manager von Norton, Avira, Bitdefender und vielen weiteren Herstellern. In welchen Varianten der Antivirus-Software die Passwort-Manager enthalten sind, unterscheidet sich je nach Anbieter. Diese Passwort-Manager speichern Ihre Kennwörter in der Cloud, haben ein Browser-Add-on, mit dem die Daten automatisch ausgefüllt werden und verschlüsseln den Passwort-Safe. Ob es Zusatzfunktionen gibt, hängt vom Anbieter ab, die meisten bieten aber zumindest eine Darkweb-Überwachung von E-Mail-Adressen an, auch wenn diese nicht Teil der Passwort-Manager, sondern ebenfalls eine Zusatzfunktion vom Virenschutz-Programm ist. Die Passwort-Manager der Antiviren-Hersteller sind zwar nicht kostenlos, aber viele Nutzerinnen und Nutzer haben eine Lizenz für ein Virenschutz-Programm, weshalb keine Zusatzkosten entstehen.

**Passwörter im Browser oder Betriebssystem speichern**

Die meisten Betriebssysteme und Browser bieten ebenfalls an, Passwörter zu speichern. So speichern Android und iOS Ihre Kennwörter auf Wunsch im Apple- oder Google-Konto. Solange man mit allen Geräten in der gleichen Hersteller-Welt ist, funktioniert das auch recht gut. Wer beispielsweise ein MacBook, ein Android-Smartphone und ein Windows-Tablet besitzt, muss sich allerdings umständlich selbst darum kümmern, dass gespeicherte Anmeldedaten auf allen Geräten verfügbar sind. Bei den Browser-Passwort-Managern sieht es ähnlich aus: Im gleichen Browser funktioniert das Synchronisieren gut, sonst nicht. Hinzu kommt bei den Browser-Passwort-Speichern, dass diese sich recht leicht knacken lassen. Zusatzfunktionen gibt es auch hier wenig. Eine Darknet-Prüfung ist zwar teilweise vorhanden, aber manchmal umständlich zu nutzen. So warnt iOS beispielsweise nicht aktiv, sondern zeigt nur in den Einstellungen an, ob die Kennwörter kompromittiert sind. Und die meisten Browser warnen nur beim Speichern der Passwörter, nicht aber beim Anmelden.

**Gratis-Versionen der Kaufprogramme**

Einige Hersteller von Kauf-Passwort-Managern bieten kostenlose Varianten der Programme an. So gibt es etwa **NordPass, LastPass, Dashlane oder Bitwarden auch als kostenlose Versionen.** Auch bei diesen Programmen sind nur die Kernfunktionen enthalten. Das heißt: Das Speichern und

automatische Ausfüllen der Passwörter funktioniert mit den Programmen gut. Zusatzfunktionen gibt es aber nicht oder nur sehr wenige und teilweise sind auch die Kernfunktionen begrenzt. So können Sie bei einigen Anbietern nur eine begrenzte Zahl von Kennwörtern speichern oder nur eine begrenzte Zahl von Geräten nutzen. Vorteil dieser Varianten: Falls Sie doch einmal auf die Kaufvarianten umsteigen wollen, ist das mit wenigen Klicks möglich. Selbst wenn Sie dabei den Anbieter wechseln, klappt das dank der Export- und Import-Funktionen problemlos.

**Wie sicher sind kostenlose Passwort-Manager?**

Wie sicher die Gratis-Passwort-Manager sind, kommt auf die Art der Passwort-Manager an:

- Browser-Passwort-Manager gelten als leicht zu knacken. Zudem sind sie sehr verbreitet, was bedeutet, dass sie eher Angriffsziel von Kriminellen werden.
- Die Accounts bei Google und Apple sind gut geschützt, aber auch sehr begehrt bei Hackern und Kriminellen. Die Gefahr besteht in diesem Fall darin: Falls es doch einmal gelingt, Ihr Konto zu knacken, haben die Angreifer nicht nur Zugriff auf Ihre E-Mail-Adressen und Zahlungsdaten, sondern auch auf alle Zugangsdaten von Ihnen.
- Programme mit lokalen Passwort-Speichern wie KeePass und Password Depot sind prinzipiell sehr sicher. Das gilt aber nur, wenn Sie ein Virenschutz-Programm nutzen. Falls Sie einen Fernzugriff auf diesen Tresor einrichten, muss dieser entsprechend gesichert werden.
- Die Varianten von Antiviren-Herstellern und die Free-Versionen der Kauf-Passwort-Manager sind sehr sicher.

**Reicht ein kostenloser Passwort-Manager aus?**

Ob man einen kostenpflichtigen Passwort-Manager braucht, hängt davon ab, wie viel Komfort und Sicherheit man haben möchte und wie gut man fehlende Funktionen ersetzen kann. Haben Sie bereits einen Dienst, der prüft, ob Ihre Zugangsdaten kompromittiert sind und schaffen Sie es, Zugangsdaten auf allen Geräten verfügbar zu haben oder brauchen Sie das vielleicht auch gar nicht, sind die sicheren kostenlosen Passwort-Manager für Sie ausreichend. Wer ohne Aufwand, Stress und Zusatzwissen einfach einen sicheren Passwort-Manager auf allen Geräten haben möchte, findet in den Kauf-Versionen eher, was er oder sie sucht. Die Kaufprogramme gibt es bereits ab knapp 1 Euro im Monat.