



Ähm ... Wie hieß das Passwort noch gleich? Dieser ganze Kuddelmuddel geht mir auf'n Keks.

Einer für alle

Passwortmanager Internetnutzer müssen sich allerlei Kennwörter merken. Ein Passwortmanager nimmt ihnen diese Last ab und erhöht die Sicherheit – einer der besten im Test macht das sogar komplett gratis.

Das häufigste Passwort in Deutschland soll „123456“ sein, gefolgt von „123456789“ und „12345678“. Jedes Jahr erheben Informatiker der Universität Potsdam diese Daten. Jedes Jahr sind die Ergebnisse ähnlich. Jedes Jahr dürfen sich Kriminelle freuen: Solche Passwörter machen es ihnen leicht, online Geschäftsunterlagen oder private Dokumente zu klauen und auf Kosten ihrer Opfer einzukaufen.

Deutlich sicherer sind lange, komplexe Passwörter. Für jedes Internetportal sollte es ein anderes sein, sonst kann ein geknacktes Kennwort dazu führen, dass Hacker mehrere Konten des Nutzers kapern.

Zusammengefasst bedeutet das, dass die meisten Internetnutzer sich eigentlich zig verschiedene, komplexe Passwörter merken müssten. Das schafft aber kein Mensch – deshalb setzen viele auf „123456“ und laden so Hacker ein.

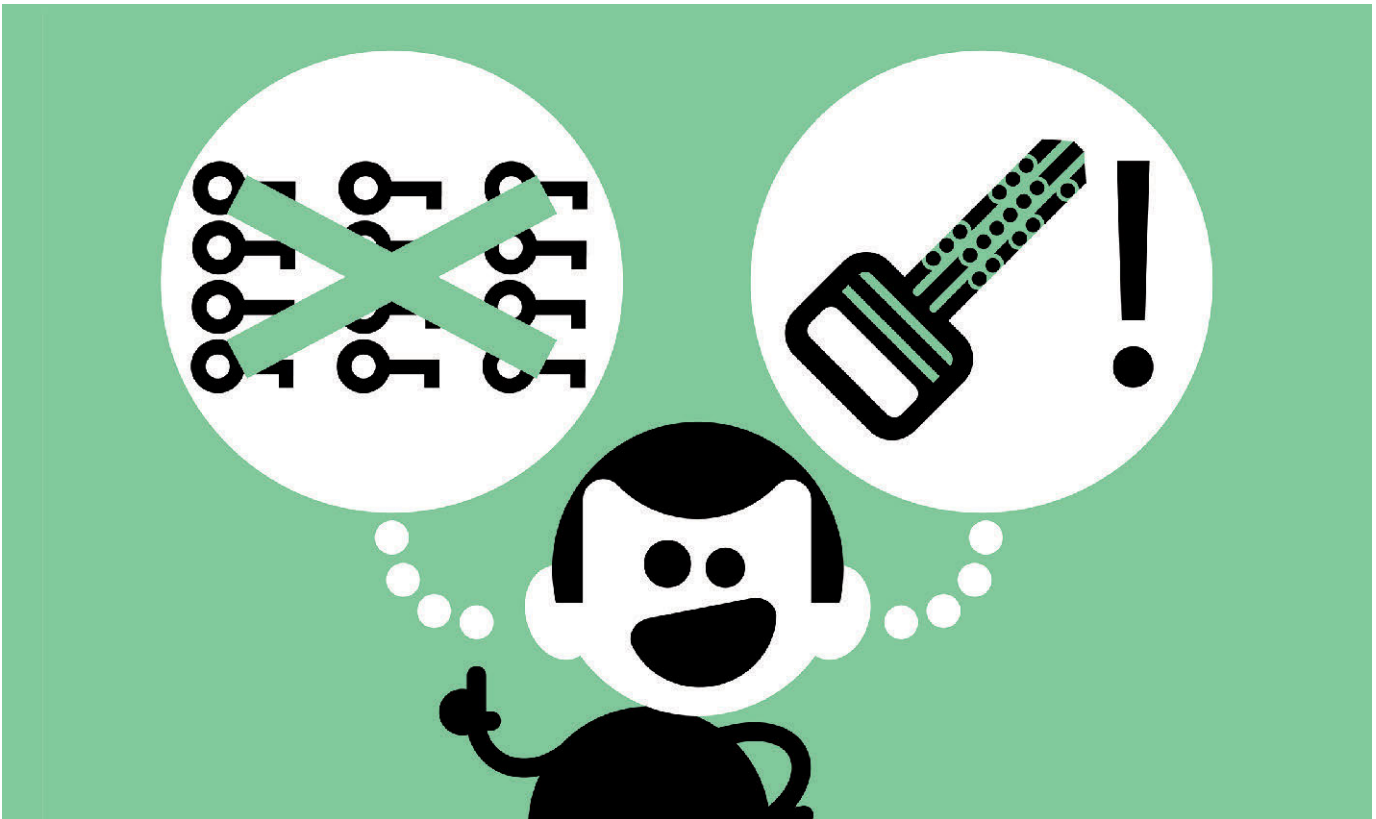
Die Rettung heißt „Passwortmanager“. Diese Programme erstellen kaum knackbare Kennwörter und sorgen zugleich dafür, dass der Nutzer sich nur noch eins merken muss: das Masterpasswort (Kasten S. 29).

Drei Manager schneiden im Test gut ab (Tabelle S. 32). Keeper Security siegt vor 1Password und KeePass. Am einfachsten zu handhaben ist das befriedigende Dashlane.

Was die Programme kosten

Alle geprüften Programme lassen sich kostenlos verwenden. Die Gratisvarianten sind aber oft mit Einschränkungen verbunden: Manche erlauben etwa nur den Gebrauch auf einem einzigen Gerät. Wer die Manager vollumfänglich und zum Beispiel auf Computer und Handy zugleich nutzen will, braucht meist ein Abo und zahlt dann zwischen 10 und 40 Euro pro Jahr. KeePass ist komplett kostenlos, das Gratispaket von Bitwarden dürfte für die meisten Nutzer ebenfalls ausreichen.

Gratis sind auch die Passwortmanagement-Funktionen der Browser Chrome,



Aah! Ein Passwort für alles – das wär was! Die Idee lass ich mir patenti... Wie, gibts schon?!?

Firefox und Safari, die wir ebenfalls getestet haben. Auf ein Qualitätsurteil für sie haben wir verzichtet, da sich die Passwort-Funktionen nicht sauber von den anderen Features der Browser trennen lassen. Aus demselben Grund konnten wir auch nicht bewerten, wie sparsam Chrome & Co Nutzerdaten erheben.

Die Browser bringen aber einen klaren Nachteil mit: Nutzer müssen sich entweder beim Surfen im Netz an einen einzigen Browser binden oder mit den Passwortmanagern mehrerer Browser jonglieren.

Unser Rat

Der Testsieger heißt Keeper Security. Das Programm kostet im Jahres-Abo 36* Euro. Ebenfalls gut sind AgileBits 1Password (38 Euro pro Jahr) und das datenschutzfreundliche, komplett kostenlose KeePass, das allerdings solides Technikwissen erfordert. Die beste Handhabung bietet das befriedigende Dashlane (40 Euro pro Jahr).

Wie Passwortmanager funktionieren

Die Manager speichern Login-Daten von Onlinekonten und geben sie – meist über ihre Browser-Erweiterungen und Apps – eigenständig in Anmeldefelder ein. Da die Programme all diese sensiblen Daten kennen, sollten Nutzer sie nur auf Geräten verwenden, die sie allein kontrollieren oder ausschließlich mit Vertrauten teilen.

Außerdem generieren die Manager komplexe Kennwörter für Online-Accounts. Da der Nutzer sich diese nicht mehr merken muss, sollten sie möglichst lang sein und keinerlei Mustern folgen. Je länger und willkürlicher, desto schwerer knackbar. Mit Ausnahme von SafeIn machen das alle geprüften Programme gut oder sehr gut.

Zusatzoptionen für mehr Sicherheit

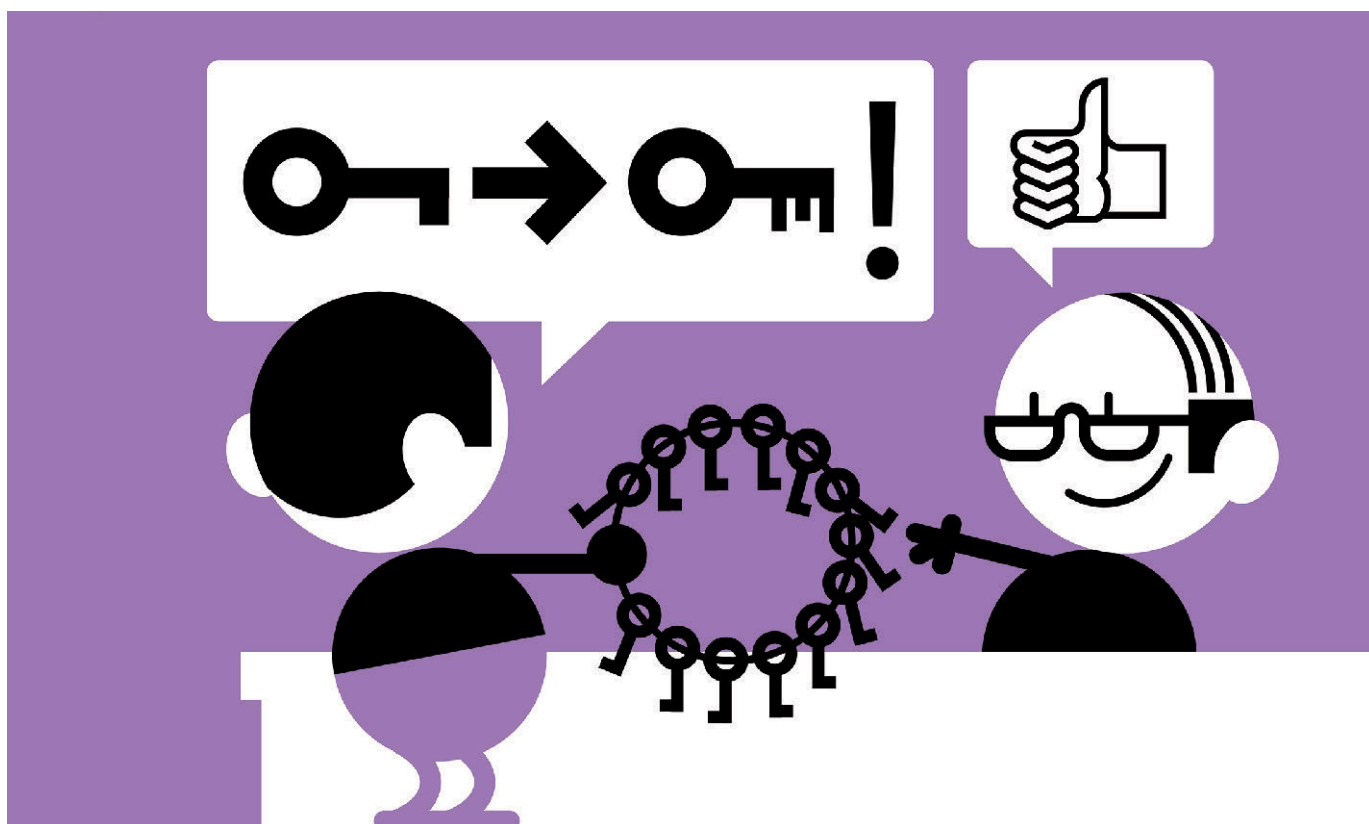
Manche Programme bringen weitere nützliche Funktionen mit: Bis auf Enpass und F-Secure bieten alle die Option, den Login zusätzlich zum Masterpasswort mit einem zweiten Faktor abzusichern, etwa dem Fingerabdruck. Hilfreich sind auch Hinweise, wie sicher ein Masterpasswort-Vorschlag des Nutzers ist. Alle geprüften Programme geben solche Einschätzungen ab. Mit der größten Vielfalt an Zusatzfunktionen punkten Keeper Security und 1Password. ►

Das richtige Masterpasswort finden

Das Masterpasswort ist wie der Schlüssel zum Schlüsselkasten. Wenn Sie es vergessen, kommen Sie nur mit großem Aufwand an Ihre Passwörter für Onlinebanking, Shopping und andere Dienste. Wählen Sie das Masterpasswort sorgfältig aus – und treffen Sie Vorkehrungen für den Fall, dass Sie es vergessen. Sie können es etwa auf einen Zettel schreiben und diesen im Banktresor lagern.

Lang, sinnlos, einprägsam. Besonders wichtig ist die Länge des Masterpassworts – wir empfehlen mindestens 20 Zeichen. Außerdem sollte es möglichst willkürlich und sinnfrei, zugleich aber gut merkbar sein. Praktisch sind etwa Nonsens-Sätze mit eingestreuten Sonderzeichen sowie Klein- und Großbuchstaben. Beispiel: „B@yerns Biber blinken * bunt3 Bingobären!“.

*) Korrigiert am 31.1.2020.



Moin! Meister, die brauch ich alle mit mehr Schnickschnack – und zwar bis gestern.

Zwei sind besonders transparent

Bei KeePass und Bitwarden trägt neben den Funktionen auch die Transparenz zur Sicherheit bei: Beide sind „Open-Source“-Programme. Im Gegensatz zu den anderen Managern im Test legen sie ihren Programmcode offen. Das ist ungewöhnlich, da der Code meist ein Geschäftsgeheimnis ist. KeePass und Bitwarden erleichtern mit ihrer Transparenz die eigene Optimierung, denn der offene Quellcode ermöglicht es zusätzlich zu internen Experten auch externen, auf Fehlersuche zu gehen.

Gut P@s5woRt will Weile haben

Passwortmanager nehmen Nutzern viel Arbeit ab. Wer all ihre Vorteile genießen will, muss aber einmal so richtig die Ärmel hochkrempeln: Für die Ersteinrichtung am Computer sollten Neukunden ein paar Stunden einplanen (siehe Anleitung S. 34). Zuerst brauchen sie eine Liste ihrer wichtigsten Onlinekonten samt Nutzernamen und Passwörtern. Dann müssen sie mit dem Manager für jedes Portal ein neues Kennwort generieren. Danach gilt es, das Programm auch auf allen anderen Geräten einzurichten, mit denen sie im Netz surfen. Die Gebrauchsanleitungen der Anbieter

helfen dabei nicht immer weiter. Manche sind nur in englischer Sprache verfügbar, was wir mit Mangelhaft bewertet haben.

KeePass erfordert Technikwissen

Besonders aufwendig ist die Ersteinrichtung von KeePass: Der Nutzer muss sich selbst um die Synchronisation kümmern – das heißt, er muss dafür sorgen, dass all seine Geräte Zugriff auf die Datei mit den Passwörtern haben. Das geht etwa, indem er die Datei bei einem Cloud-Dienst (siehe test 5/2019) hochlädt und seine Geräte mit diesem Dienst verbindet.

Die Nutzung von KeePass wird zusätzlich dadurch erschwert, dass die offizielle Software nur für Windows erhältlich ist. Bei Android, iOS und macOS sind Nutzer auf Lösungen von Drittanbietern angewiesen. Die offizielle KeePass-Seite bietet eine ganze Reihe solcher Gratis-Programme unter keepass.info/download.html.

Wir haben im Test KeePass2Android und KeePass Touch für iOS verwendet. Wie gut andere Drittanbieter-Apps funktionieren, lässt sich daraus nicht ableiten. Klar ist aber, dass sich KeePass aufgrund dieser Hürden primär für Nutzer mit solidem Technikwissen eignet.

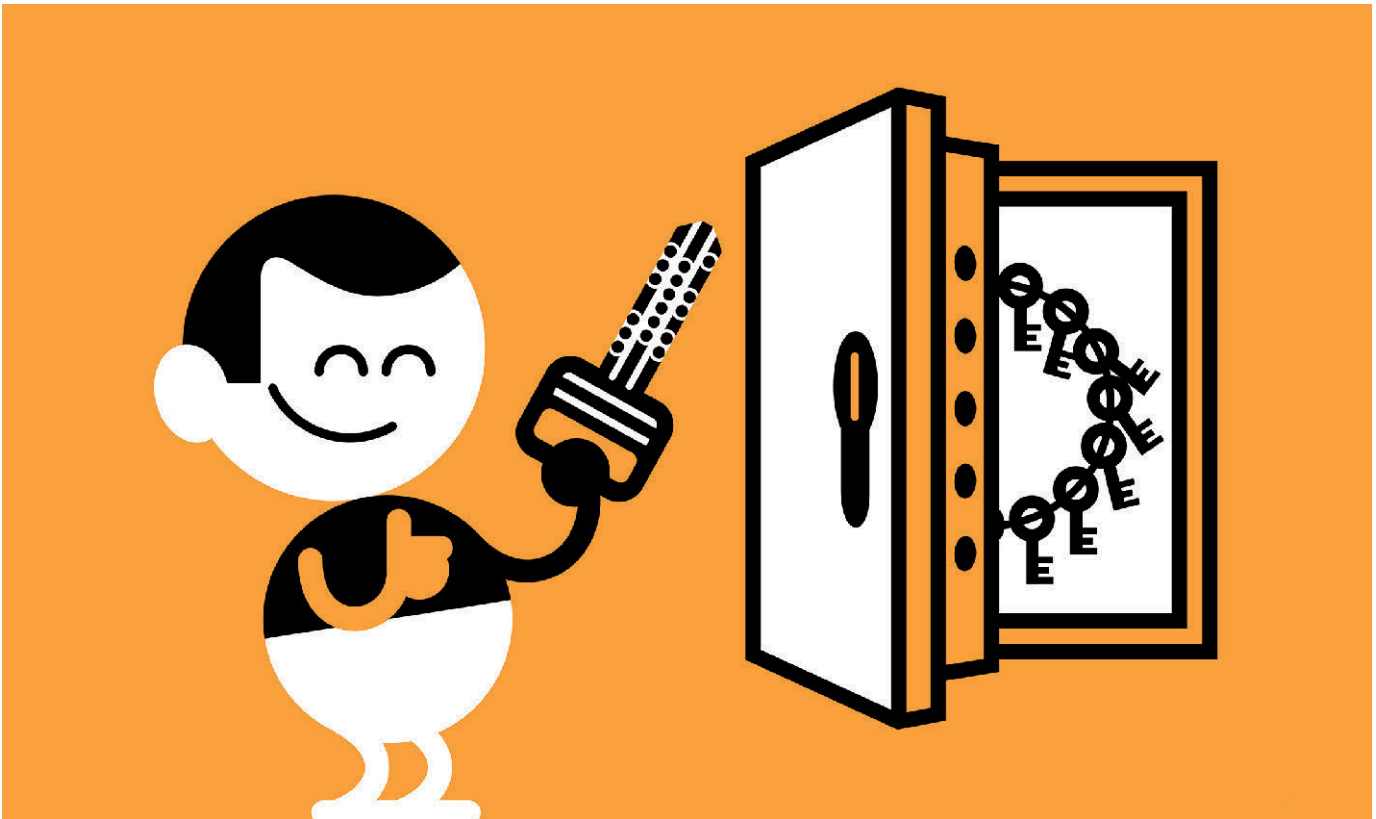
Nur KeePass ohne Mängel im Papier

In anderen Prüfpunkten hebt sich KeePass wiederum positiv von der Konkurrenz ab: Das betrifft vor allem das Vertragswerk. KeePass kommt als einziger Dienst im Test ohne Defizite in der Datenschutzerklärung und den Nutzungsbedingungen aus.

Fast alle anderen Anbieter haben sehr deutliche Mängel. In vielen Fällen besteht das Problem schlicht darin, dass die Texte nur auf Englisch vorliegen – das ist nicht verbraucherfreundlich, gerade bei komplexen juristischen und technischen Erklärungen. Zusätzlich stießen wir in vielen Texten auf Klauseln, die Nutzer benachteiligen – darunter waren etwa schwammige Beschreibungen und Fälle, in denen Anbieter sich vorbehalten, ihren Dienst kurzfristig einzustellen.

Vorsicht vor dem Super-GAU

Die Vorteile von Passwortmanagern liegen auf der Hand: mehr Sicherheit, weniger Stress. Sie können aber auch zu Problemen führen. So erlauben Enpass, KeePass, Kaspersky und SafeIn Masterpasswörter mit weniger als fünf Zeichen. Das halten wir für zu unsicher, wir werteten die Manager daher im Urteil Sicherheitsfunktionen ab. ►



Hach! So, alles palletti. Ich muss nüschts mehr inner Birne behalten und Hacker jucken mich auch nich mehr.

Sieben Tipps für noch mehr Sicherheit

Neben Passwortmanagern haben Sie weitere Optionen, um Ihre Kennwörter zu schützen.

Geräte sichern. Sperren Sie den Zugang zu Ihren Computern und Handys – sonst können Fremde trotz Passwortmanager in manche Ihrer Onlinekonten eindringen und Daten stehlen. Die sicherste Methode ist der Fingerabdruck, Passwörter sind oft eine bessere Wahl als Pin-Codes.

E-Mail-Konto schützen. Fast jedes Mal, wenn Sie ein Passwort zurücksetzen, weil Sie es vergessen haben, erhalten Sie eine E-Mail vom jeweiligen Portal. Kann ein Angreifer in Ihr Postfach eindringen, hat er Zugriff auf solche Mails und kann all Ihre Passwörter ändern. Das Kennwort für Ihr

E-Mail-Konto sollte daher besonders stark und im Idealfall mit einem zweiten Login-Faktor verknüpft sein.

Hack-Check. Auf Seiten wie haveibeenpwned.com oder sec.hpi.de/ilc können Sie prüfen, ob Ihre Nutzerkonten von Hacks betroffen sind. Falls ja, sollten Sie alle mit dem jeweiligen E-Mail-Konto verbundenen Passwörter ändern.

Vorsicht vor Phishing. Öffnen Sie keine Links in Mails von Fremden. Kriminelle versuchen, Sie damit auf gefälschte Seiten zu locken, die aussehen wie bekannte Websites. Dort sollen Sie Ihre Login-Daten eingeben – die Täter greifen sie dann ab.

Achtung bei Browsern.

Wenn Sie sich auf Websites anmelden, fragt der Browser oft, ob er Ihre Login-Daten speichern soll. Das ist bequem, aber riskant: Haben Fremde, Kollegen oder Mitbewohner Zugriff auf den Computer, können sie die Passwörter mitunter im Klartext einsehen. Schützen Sie die Kennwörter mit einem Masterpasswort oder verzichten Sie ganz darauf, Passwörter im Browser zu speichern. In Chrome lässt sich die Funktion so deaktivieren: Einstellungen > Auto-Fill > Passwörter > Option „Speichern von Passwörtern anbieten“ abschalten. Im selben Menü können Sie auch bereits gespeicherte Passwörter löschen.

Alte Konten löschen.

Falls Sie bestimmte Konten nicht mehr nutzen, sollten Sie sie löschen. Je weniger Online-Accounts Sie haben, desto geringer ist die Gefahr, Opfer von Hacks zu werden. Die Website justdelete.me bietet Hinweise für zahlreiche Internetportale, wie sich dortige Accounts rasch entfernen lassen.

Ändern ist out. Früher rieten Experten dazu, Passwörter regelmäßig zu ändern. Inzwischen gilt aber der Ratschlag, lieber einmal ein richtig starkes Kennwort zu wählen und dabei zu bleiben, solange es nicht gehackt wird.

Die größte Katastrophe wäre, das Masterpasswort zu vergessen. Wem das passiert, der verliert den Zugang zu seinem digitalen Leben. Nur 1Password, F-Secure, KeePass, Keeper Security, LastPass und True Key sowie die drei geprüften Browser bieten Optionen, den Zugriff wiederzuerlangen. Das Masterpasswort muss daher sehr gut durchdacht sein – Nutzer sollten es zudem aufschreiben und an einem sicheren Ort aufbewahren (siehe Kasten S. 29).

Von Passwortmanagern abhängig

Ein weiteres Problem ist der Autonomieverlust: Wer sich einmal entschieden hat, einen Passwortmanager zu verwenden, macht sich davon abhängig. Ist das Pro-

gramm mal nicht verfügbar – etwa auf dem Bürorechner, dem Tablet von Freunden, im Internetcafé oder nach einem Geräteverlust im Urlaub –, kann sich der Nutzer in keines seiner Onlinekonten einloggen, da er die vom Manager generierten, komplexen Passwörter ja gar nicht kennt.

Bitwarden, Kaspersky, Keeper Security und LastPass ermöglichen es in solchen Fällen, sich auf der Anbieter-Website mit dem Masterpasswort anzumelden, um an die eigenen Kennwörter ranzukommen. Bei Chrome und Safari klappt das ebenfalls – mithilfe des Account-Passworts.

Wählt der Nutzer ein anderes Programm, muss er selbst für den Ernstfall vorsorgen: Er kann zum Beispiel die verschlüsselte


Datei mit den Passwörtern auf einem USB-Stick speichern und diesen überallhin mitnehmen. Oder er übergibt einem Vertrauten eine Kopie der Datei und lässt sich diese im Notfall zuschicken.

Eine Liste mit im Klartext notierten Passwörtern mitzuführen, wäre hingegen sehr riskant: Fällt die Liste Fremden in die Hände, sind sämtliche Onlinekonten des Nutzers in Gefahr. Der einzige Ort, an dem solche Listen eine Existenzberechtigung haben, sind Tresore mit einem komplexen Zahlencode als „123456“. ■

Schritt für Schritt. Wie Sie Passwortmanager einrichten und damit Kennwörter ändern, lesen Sie auf S. 34–35. ►►



Passwortmanager: 1Password und Keeper Security haben die besten Sicherheitsfunktionen

		Passwortmanager						
Produkt		Keeper Security Keeper	AgileBits 1Password	KeePass ⁴⁾ Password Safe, Keepass2 Android, KeePassTouch, KeePass Tusk	Dashlane Premium	LastPass Premium	8bit Solutions Bitwarden Password- Manager Free	Kaspersky Password Manager
Preis pro Jahr ca. (Euro)		36 ¹⁾ 11)	38 ²⁾	Kostenlos	40 ⁵⁾	39 ⁵⁾	Kostenlos	14 ¹⁾
 test - QUALITÄTSURTEIL	100 %	GUT (2,4)	GUT (2,5)	GUT (2,5)	BEFRIEDIGEND (2,7)	BEFRIEDIGEND (2,8)	BEFRIEDIGEND (2,9)	BEFRIEDIGEND (2,9)
Sicherheitsfunktionen	30 %	sehr gut (1,0)	sehr gut (0,9)	befried. (2,9)	gut (1,9)	gut (1,6)	sehr gut (1,3)	ausreich. (3,6)
Anforderungen an Masterpasswort		++	++	⊖ ^{*)}	+	++	++	⊖ ^{*)}
Automatische Passwortgenerierung		++	++	++	+	+	++	+
Sicherheitskonzept		++	++	+	++	++	++	++
Handhabung	30 %	gut (2,2)	gut (2,5)	befried. (3,4)	gut (1,7)	gut (2,5)	befried. (3,0)	gut (2,1)
Gebrauchsanleitung und Hilfen		⊖	— ^{*)} 3)	— ^{*)} 3)	+	○	— ^{*)} 3)	++
Installation und Inbetriebnahme		○	+	⊖	+	+	+	+
Täglicher Gebrauch/Praxistest Websites		+ / ++	+ / +	+ / ○	+ / ++	+ / ○	+ / ○	+ / +
Funktionsumfang	25 %	gut (1,8)	gut (1,8)	gut (1,9)	gut (2,1)	gut (2,1)	gut (2,2)	gut (2,1)
Basisschutz persönlicher Daten	15 %	befried. (3,5)	befried. (3,5)	sehr gut (1,0)	befried. (3,5)	befried. (3,5)	befried. (3,5)	sehr gut (1,0)
Sparsames Erheben von Nutzerdaten		○	++	++	○	○	++	++
Mängel in der Datenschutzerklärung		sehr deutlich ^{*)}	sehr deutlich ^{*)}	keine	sehr deutlich ^{*)}	sehr deutlich ^{*)}	sehr deutlich ^{*)}	gering
Mängel in den Nutzungsbedingungen/AGB	0 %	sehr deutlich ^{*)}	sehr deutlich ^{*)}	keine	sehr deutlich ^{*)}	sehr deutlich ^{*)}	sehr deutlich ^{*)}	sehr deutlich ^{*)}
Technische Merkmale								
Erweiterung für Chrome/Firefox/Opera		■/■/■	■/■/■	■/■/■	■/■/□	■/■/■	■/■/■	■/■/■
Erweiterung für Edge/Internet Explorer/Safari		■/■/■	■/□/■	■/■/■	■/■/■	■/□/■	■/□/■	■/■/■
Import aus/Export zu anderen Passwortmanagern		■/■	■/■	■/■	■/■	■/■	■/■	■/■

Bewertungsschlüssel der Prüfergebnisse:

++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5). ○ = Befriedigend (2,6–3,5).

⊖ = Ausreichend (3,6–4,5). — = Mangelhaft (4,6–5,5).

Bei gleichem Qualitätsurteil Reihenfolge nach Alphabet.

*) Führt zur Abwertung (siehe „So haben wir getestet“ auf Seite 33).

■ = Ja. □ = Nein.

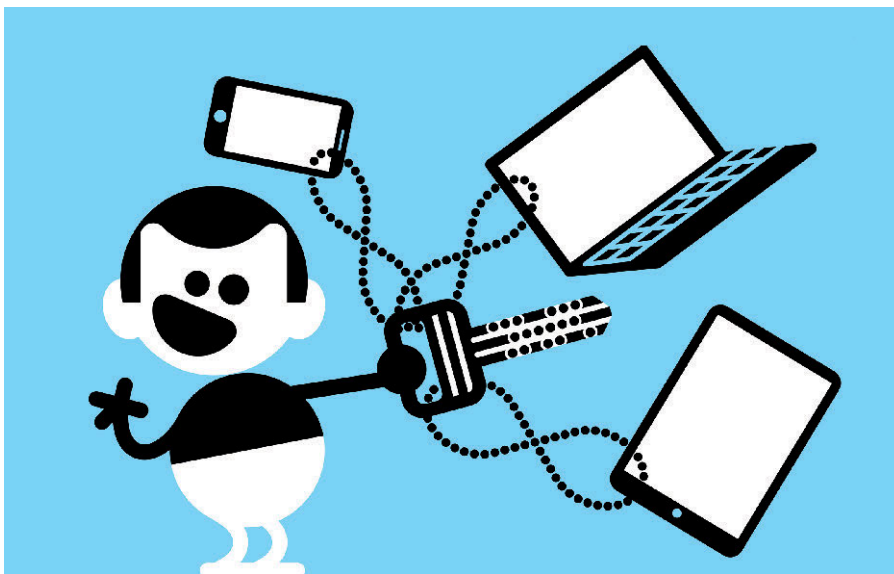
Mängel in den Datenschutzerklärungen und Nutzungsbedingungen/AGB: keine, sehr gering, gering, deutlich, sehr deutlich.

1) Jährliche Kosten für Desktopversion laut Anbieter-Webseite; dafür müssen im Bestellprozess zwei vom Anbieter vorausgewählte Optionen abgewählt werden: „10 GB Cloudspeicher“ und „BreachWatch“ (Korrigiert am 31.1.2020). Die mobile App ist kostenlos.

2) Jährliche Kosten für geräteübergreifende Nutzung laut Anbieter-Webseite. 3) Keine deutsche Gebrauchsanleitung.

4) Offizielles Programm nur für Windows erhältlich. Wir testeten zusätzlich exemplarisch KeePass 2.4.3 für macOS (über mono), KeePass2Android, KeePass Touch für iOS und die Chrome-Erweiterung KeePass Tusk.

5) Jährliche Kosten für Premium-Desktopversion laut Anbieter-Webseite. Die mobile App ist kostenlos.



Tschakka! Noch fix den ganzen Krimskrams zusammentüdeln – und aus die Maus!



				In Browser integrierte Passwortmanager		
McAfee True Key Premium	Sinew Enpass Premium	F-Secure Key Premium	SafelInCloud ⁷⁾	Apple Safari mit iCloud-Schlüsselbund	Google Chrome Browser	Mozilla Firefox Browser
20 ⁵⁾	16 ⁶⁾	30 ¹⁾	4 ⁸⁾ Einmalig	Kostenlos	Kostenlos	Kostenlos
BEFRIEDIGEND (3,2)	BEFRIEDIGEND (3,5)	AUSREICHEND (3,6)	AUSREICHEND (3,7)	NICHT VERGEBEN⁹⁾	NICHT VERGEBEN⁹⁾	NICHT VERGEBEN⁹⁾
sehr gut (1,5)	befried. (3,0)	gut (2,1)	ausreich. (3,6)	sehr gut (1,3)	gut (1,6)	ausreich. (4,0)
+	⊖ ^{*)}	○	⊖ ^{*)}	++	++	+
++	++	++	○	++	++	++
+	+	○	++	+	○	⊖ ^{*)10)}
befried. (3,1)	befried. (3,2)	befried. (3,4)	befried. (3,2)	gut (1,9)	gut (1,8)	gut (2,2)
○	— ^{*)3)}	⊖	— ^{*)3)}	○	○	+
○	+	○	+	++	++	++
○/○	+/○	○/⊖	+/○	+/+++	+/+++	+/+
befried. (3,0)	gut (2,3)	ausreich. (3,8)	befried. (2,6)	ausreich. (3,8)	befried. (3,3)	ausreich. (4,5)
befried. (3,5)	befried. (3,5)	befried. (3,3)	befried. (3,5)	Nicht bewertet	Nicht bewertet	Nicht bewertet
○	++	○	++	Nicht bewertet	Nicht bewertet	Nicht bewertet
sehr deutlich ^{*)}	sehr deutlich ^{*)}	deutlich ^{*)}	sehr deutlich ^{*)}	sehr deutlich	sehr deutlich	sehr deutlich
sehr deutlich^{*)}	sehr deutlich^{*)}	sehr deutlich^{*)}	sehr deutlich^{*)}	sehr deutlich	sehr deutlich	sehr deutlich
■/■/□	■/■/■	■/■/□	■/■/■	Entfällt	Entfällt	Entfällt
■/□/□	■/□/■	□/□/□	■/□/□	Entfällt	Entfällt	Entfällt
■/■	■/■	■/■	■/■	■/□	■/■	■/□

6) Preis für die mobilen Apps. Unbeschränkte Desktopversion kostenlos verfügbar.

7) Getestet mit der „Individual Pro“-Version für die mobilen Apps.

8) Einmalige Kosten für mobile „Individual Pro“-Version laut Anbieter-Webseite. Die Desktopversion ist kostenlos.

9) Ein test-Qualitätsurteil haben wir nicht vergeben, da wir nicht alle Funktionen der Browser getestet haben, sondern nur das Passwortmanagement.

10) Loggt sich der Nutzer in den Browser ein, werden seine von Firefox gespeicherten Passwörter auf den Computer übertragen.

Verwenden andere Nutzer dasselbe Gerät unter demselben Geräteprofil, können sie die Passwörter unter Umständen im Klartext einsehen.

11) Korrigiert am 31.1.2020.

So haben wir getestet

Im Test: 10 plattformübergreifende Passwortmanager ohne Funktionseinschränkungen sowie KeePass und 3 verbreitete Browser. Die Preise erhoben wir im Dezember 2019 auf den Anbieter-Websites.

Untersuchungen: Eine vollständige Beschreibung der Testmethodik finden Sie im Internet unter test.de/pwm/methodik.

Sicherheitsfunktionen: 30 %

Wir prüften, welche **Anforderungen** die Programme an das **Masterpasswort** stellen und wie sicher die Vorschläge der **automatischen Passwortgenerierung** sind. Beim **Sicherheitskonzept** prüften wir zum Beispiel Schutzmaßnahmen gegen Angriffe.

Handhabung: 30 %

Drei geschulte Prüfer bewerteten die **Gebrauchsanleitungen und Hilfen**, die **Installation und Inbetriebnahme** der Programme und den **täglichen Gebrauch** (z.B. Entsperren, Erstellen neuer Einträge). Hinzu kam ein **Praxistest auf Websites**: Wir prüften dabei, ob die automatische Eingabe der Anmeldedaten klappt.

Funktionsumfang: 25 %

Wir prüften vorhandene Zusatzfunktionen.

Basisschutz persönlicher Daten: 15 %

Wir analysierten den Datenstrom der mobilen Apps und beurteilten, ob die Anbieter beim **Erheben von Nutzerdaten** sparsam vorgehen. Ob die Empfänger der Daten diese weiterverarbeiten oder weitergeben, können wir nicht untersuchen. Ein Jurist prüfte die **Datenschutzerklärung auf Mängel**, etwa unzureichende Angaben über die Weitergabe von Daten an Dritte.

Mängel in Nutzungsbedingungen/AGB: 0 %

Ein Jurist prüfte die Nutzungsbedingungen bzw. AGB der Anbieter auf unzulässige Klauseln, die Nutzer benachteiligen.

Abwertungen

Waren die Anforderungen an das Masterpasswort ausreichend, werteten wir die Sicherheitsfunktionen um eine halbe Note ab. War das Sicherheitskonzept ausreichend, konnten die Sicherheitsfunktionen nicht besser sein. Waren Gebrauchsanleitungen und Hilfen mangelhaft, werteten wir die Handhabung um eine halbe Note ab. Hatte die Datenschutzerklärung deutliche oder sehr deutliche Mängel, werteten wir den Basisschutz persönlicher Daten um 0,3 bzw. 0,5 Noten ab – zudem konnte das übergeordnete Urteil dann nicht besser als befriedigend sein. Hatten die Nutzungsbedingungen/AGB sehr deutliche Mängel, werteten wir das test-Qualitätsurteil um eine halbe Note ab.

In fünf Schritten zu mehr Komfort und Sicherheit

Aller Anfang ist schwer?
Unsere Anleitung zeigt, wie Sie einen Passwortmanager in wenigen Schritten einrichten.

1 Nutzerkonto anlegen

Erstellen Sie ein Nutzerkonto für den Passwortmanager Ihrer Wahl, indem Sie sich per Computer auf der Website des Anbieters registrieren. Bei KeePass und Enpass entfällt dieser Schritt.

2 Programm am Computer einrichten

Laden Sie von der Anbieter-Website die Installationsdatei des Managers auf Ihren Computer herunter und installieren Sie das Programm. Wählen Sie ein Masterpasswort. Installieren Sie anschließend auch die Browser-Erweiterung Ihres Managers in allen Browsern, die Sie verwenden. Legen Sie in den Browser-Einstellungen fest, dass sich künftig nicht mehr der Browser, sondern Ihr neuer Passwortmanager standardmäßig um Ihre Login-Daten kümmern soll. Schließen Sie alle Browser-Fenster und starten Sie den Browser neu.

3 App auf dem Handy installieren

Richten Sie die App Ihres Passwortmanagers auf Ihrem Handy und, falls vorhanden, Ihrem Tablet ein.

4 Die wichtigsten Portale besuchen

Rufen Sie die Websites und Apps auf, die für Sie besonders wichtig sind, und melden Sie sich dort in Ihren jeweiligen Konten an. Beim Login fragt Ihr Passwortmanager, ob er die Anmeldedaten speichern soll. Die Entscheidung hängt davon ab, ob es Ihnen beim Nutzen des Managers allein um **mehr Komfort (5a)** oder zusätzlich auch um **mehr Sicherheit (5b)** geht. Um Anmeldedaten für weniger wichtige Portale kümmern Sie sich einfach, wenn Sie die jeweilige Plattform das nächste Mal besuchen – Ihr Passwortmanager wird Sie danach fragen.

5a Für mehr Komfort sorgen

Haben Sie sich für einen Passwortmanager entschieden, damit Sie sich Ihre Login-Daten nicht mehr merken müssen, dann bestätigen Sie, dass der Manager diese Daten speichern soll. Ab dem nächsten Login sollte er sie automatisch eingeben. Sie haben es geschafft!

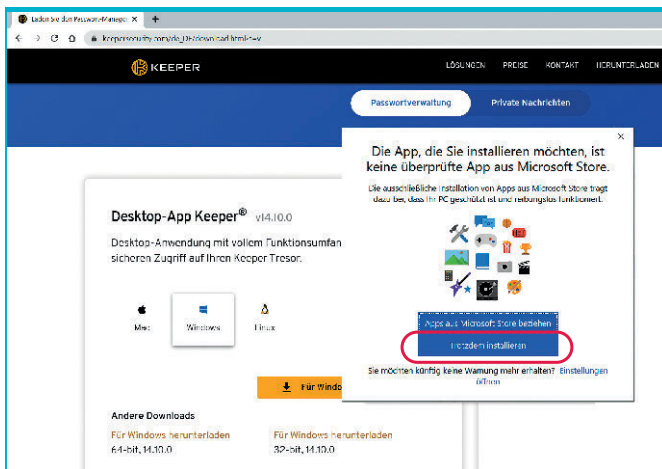
5b Für mehr Sicherheit sorgen

Haben Sie sich für einen Passwortmanager entschieden, um auch die Sicherheit Ihrer Passwörter zu stärken, dann sollten Sie das Speichern Ihrer Login-Daten an dieser Stelle ablehnen. Sie müssen nämlich zunächst mal Ihre bisherigen Passwörter durch maschinell generierte ersetzen, damit Ihr Sicherheitsniveau steigt.

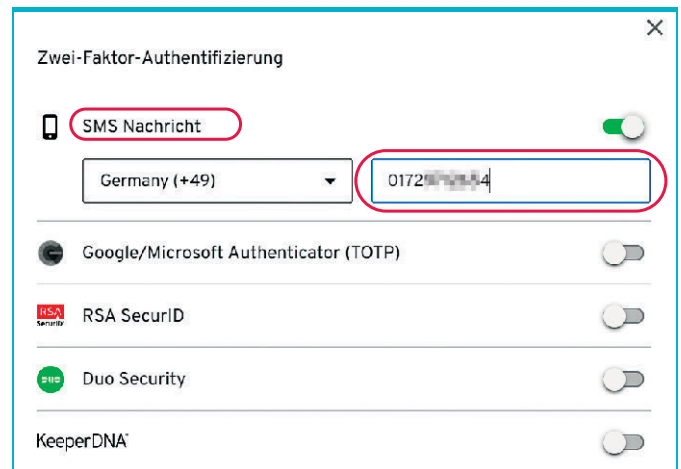
Dazu suchen Sie auf den von Ihnen genutzten Internetportalen nach der Möglichkeit, Ihr Passwort zu ändern. Geben Sie Ihr altes Kennwort manuell in das dafür vorgesehene Feld ein. Sobald Sie in das Feld für das neue Passwort klicken, sollte ein Symbol Ihres Passwortmanagers erscheinen. Der Manager kann nun ein neues Kennwort für Sie generieren. Bestätigen Sie es oder passen Sie es, falls nötig, an die Passwortvorgaben der Seite an.

Speichern Sie das neue Kennwort sowohl im jeweiligen Internetportal als auch in Ihrem Passwortmanager. Ab dem nächsten Login sollte der Manager Sie automatisch anmelden. Sie haben es geschafft!

Tipp: Auf manchen Internetseiten treten beim Ändern des Passworts Probleme auf – die lassen sich aber lösen (siehe rechts). ■



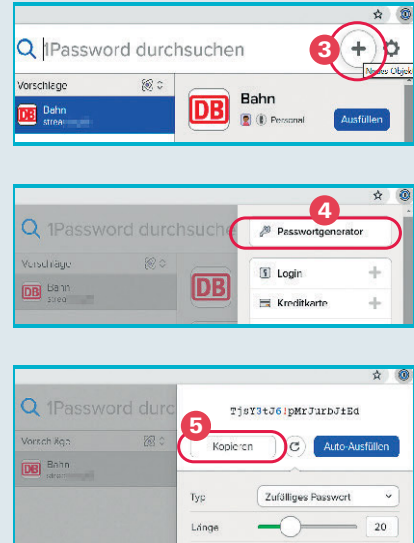
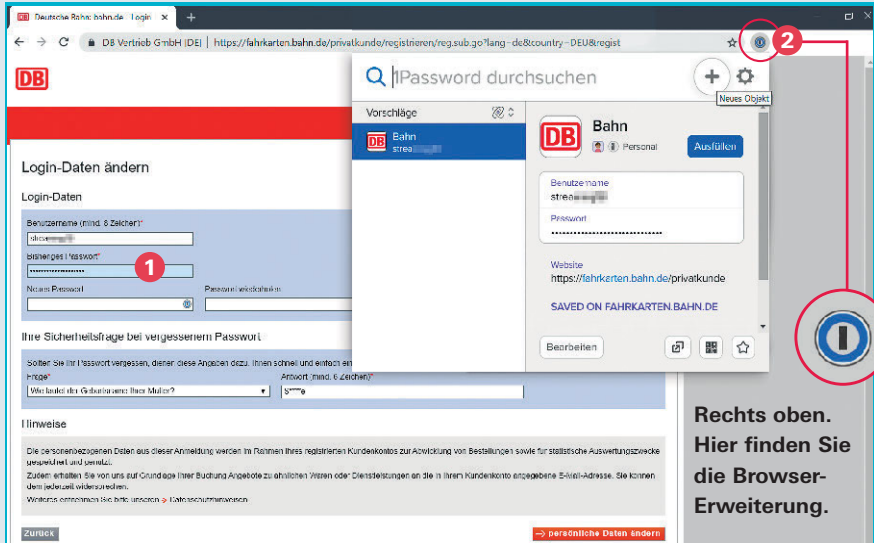
Trotzdem installieren. Diese Warnung können Sie ignorieren, wenn Sie Ihren Manager von der Anbieterseite herunterladen.



Zweiter Faktor. Noch sicherer sind Sie, wenn Sie zum Beispiel Ihre Handynummer mit dem Passwortmanager verknüpfen.

Der Widerspenstigen Zähmung

Manche Seiten zicken etwas, wenn Sie per Passwortmanager Ihr Kennwort ändern wollen. Mit ein paar Handgriffen lässt sich dieses Problem aber lösen.



Wenn Sie Ihre Passwörter stärken wollen, sollten Sie selbstgemachte Kennwörter durch maschinell generierte ersetzen. Doch im Test stellten wir fest, dass das mitunter gar nicht so leicht ist: Manche Seiten – etwa bahn.de, ebay.de oder kicker.de – arbeiteten mit einigen Passwortmanagern nicht besonders gut zusammen.

Passwort händisch wiederholen. Ein Fehler trat besonders häufig auf: Beim Ändern des Passworts muss das neue Kennwort auf vielen Portalen zweimal eingegeben werden. Bei suboptimal programmierten Seiten trug der Manager das neue Passwort aber versehentlich in das Feld für das alte Kennwort ein. Sie erkennen das im Normalfall daran, dass plötzlich ein Passwort in diesem Feld angezeigt wird, das länger ist als ihr bisheriges Kennwort.

Menschliche Nachhilfe für die Software. Ohne manuelles Eingreifen war es den Managern in solchen Fällen nicht möglich, das Passwort zu ändern. Dieses Problem lässt sich lösen, indem Sie zunächst Ihr altes Passwort erneut händisch eingeben. Dann können Sie das vom Manager generierte neue Passwort aus dem Programm herauskopieren und auf der Website in die

Felder für das neue Passwort einfügen. Wie das funktioniert, lesen Sie in der folgenden Anleitung.

Schritt für Schritt. Am Beispiel von 1Password und dem Browser Chrome zeigen wir, wie Sie auf der Website der Deutschen Bahn Ihr Kennwort ändern.

- 1 Bisheriges Passwort manuell ins entsprechende Feld eingeben.
- 2 Browser-Erweiterung von 1Password rechts oben im Browser aufrufen. Falls nötig, Masterpasswort eingeben.
- 3 Auf das Pluszeichen klicken.
- 4 Passwortgenerator wählen.
- 5 Unter dem Passwortvorschlag auf „Kopieren“ klicken.
- 6 Auf der Bahn-Seite mit der linken Maustaste in das Feld fürs neue Passwort klicken, rechte Maustaste drücken und „Einfügen“ wählen.
- 7 Feld „Passwort wiederholen“ ebenso durch „Einfügen“ befüllen.
- 8 Auf „In 1Password speichern“ klicken.
- 9 Mit „Update“ bestätigen.
- 10 Button „persönliche Daten ändern“ auf der Bahn-Seite anklicken.

