So geht's leichter...

Alle Passwörter im Griff

- Gute Passwörter erstellen
- Gefährdete Konten erkennen
- Passwörter merken im Browser
- Arbeiten mit Passwort-Manager
- Online-Konten zusätzlich sichern

Inhalt

So geht’s leichter | Passwörter im Griff

So geht’s leichter | Passwörter im Griff

Passwörter im Griff

Jedes Online-Konto, ob nun für den Zugang zu Windows 10, einen Online-Shop, Ihre Banking-Software oder das Social Media Konto, benötigt einen Anmeldenamen (Benutzername) und ein Passwort.

Die erste Komponente – der Benutzername – ist häufig automatisch die E-Mail-Adresse, die Sie zur Kommunikation verwenden.

Damit bleibt dann „nur“ das Passwort der wirklich geheime und geheim zu haltende Teil für den Kontozugang.

Grund genug, bei der Auswahl des Passworts etwa Zeit zu investieren und ein möglichst sicheres Passwort zu vergeben.

Wir zeigen Ihnen in diesem Report alles rund um den sicheren Umgang mit Passwörtern. Wie Sie Ihre Passwörter selbst so festlegen, dass Sie sie sich gut merken können (auch mit technischen Hilfsmitteln), gleichzeitig aber auch von Unbefugten schwer zu erraten sind. Möglichkeiten, kompromittierte Passwörter zu erkennen und schnell zu ändern. Hilfsmittel, wie Sie Passwörter erzeugen und dann sicher aufbewahren können und vieles mehr.

So geht's leichter | Passwörter im Griff

Das Einmaleins der Passwörter

Ein gutes und solides Passwort zu finden, ist keine einfache Aufgabe. Wird man aufgefordert, sich mal wieder schnell ein Passwort einfallen zu lassen, neigen viele Menschen – aus Bequemlichkeit! – dazu, ein naheliegendes Passwort zu wählen. Eins, das sich leicht merken lässt. Oder sogar immer dasselbe.

Doch das ist nun wirklich keine gute Idee. Aus einem ganz einfachen Grund: Gelingt es jemandem, etwa einen Hacker oder Cyber-Kriminellen, sich unbefugt Zugang zu einem der Konten mit diesem Passwort zu verschaffen (etwa durch Ausspionieren, oder indem ein gehacktes Konto im Darknet „gekauft" wird), hat diese Person nicht nur Zugriff auf dieses Konto, sondern auch auf alle weiteren Konten, die dasselbe Passwort haben. So etwas probieren Hacker/Cyberkriminelle gerne aus!

Das gilt es also unbedingt zu vermeiden. Die gute Nachricht: Es gibt einige Hilfsmittel, mit denen Sie die Passwortvergabe strukturierter angehen können.

Das sichere Passwort

Eigentlich ist der Begriff irreführend. Ein „sicheres" Passwort ist ebenso theoretisch wie ein Perpetuum Mobile, denn mit genügend Rechenpower und Zeit lässt sich wohl jedes Passwort irgendwann herausfinden. Sie können den Aufwand aber zumindest so hochtreiben, dass die Wahrscheinlichkeit, dass das passiert, gegen Null geht.

So geht’s leichter | Passwörter im Griff

Wenn Sie jetzt der Meinung sind, dass eine Mahnung nach guten Passwörtern doch sinnlos ist und schon durch den gesunden Menschenverstand erledigt sein sollte: Grundsätzlich haben Sie Recht.

Allerdings eben nur grundsätzlich. Man mag es kaum glauben, aber die Anwender sind oft allzu sorglos.

Das Hasso-Plattner-Institut bringt regelmäßig eine Übersicht der beliebtesten Passwörter heraus, die Sie für 2019 unter https://hpi.de/pressemitteilungen/2019/die-beliebtesten-deutschen-passwoerter-2019.html finden.

Ganz vorne (und das leider schon seit Jahren immer wieder): **123456**, **123456789** und **12345678**. Kombinationen von Ziffern, die ein Angreifer als allererstes ausprobieren wird!

Was ist nun ein sicheres Passwort? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt unter https://www.bsi-fuer-buerger.de im Bereich **PASSWORT** einige Hinweise.

1. **ES SOLLTE EINFACH ZU MERKEN SEIN:** Je schwerer ein Passwort zu merken ist, desto höher ist die Wahrscheinlichkeit, dass sie es sich aufschreiben. Das widerspricht dem Anspruch, dass es nur Ihnen selbst bekannt sein soll. Das so beliebte kleine, gelbe PostIt als Zwischenspeicher ist eben nicht sicher!

So geht's leichter | Passwörter im Griff

2. **Es sollte mindestens 8 Zeichen haben:** Mehr (an Buchstaben) ist hier tatsächlich mehr (an Sicherheit). Bei den Passwörtern für Ihr WLAN werden gar 20 Zeichen empfohlen.

3. **Nutzen Sie Sonderzeichen, Groß- und Kleinschrift und Ziffern:** Je komplexer das Passwort ist, desto schwerer ist er herauszubekommen. Wichtig dabei auch:

4. **Verwenden Sie keine über sie bekannten oder herauszufindenden Daten als Passwort:** Namen von Familienmitgliedern, Haustieren, Freunden, Geburtstage, Hochzeitstage etc. eignen sich nicht als Passwort. Auch keine Wörter, die in einem Wörterbuch vorkommen, oder Zeichen- oder Ziffernfolgen, die auf- oder absteigend sind wie 123456 oder abcdef – siehe die eben angesprochene Liste der beliebtesten Passwörter.

Wichtig

Passwörter aus dem Wörterbuch auszuwählen, ist keine gute Idee: So genannte Wörterbuch-Angriffe (Dictionary Attacks) sind nicht selten: Automatisiert wird der Benutzername immer wieder angemeldet, das Passwort wird eines nach dem anderen aus einem Wörterbuch genommen. Bei den heutigen Rechenkapazitäten ist es nur eine Frage der (kurzen) Zeit, bis das richtige Passwort erraten wäre!

Eselsbrücken helfen

Passwörter müssen nicht lesbar sein oder aus tatsächlich vorhandenen Begriffen bestehen, damit Sie sich daran erinnern können. Der Ausgangspunkt für ein gutes Passwort kann beispielsweise ein für Sie ganz persönlich leicht zu merkender Satz oder eine Zeile aus einem Lied sein.

So geht's leichter | Passwörter im Griff

„Ich habe im Sommer 2018 den Motorradführerschein gemacht!" beschreibt ein Ereignis, an das Sie sich sicherlich noch lange erinnern werden.

Nehmen Sie davon nur die Anfangsbuchstaben (unter Beachtung der Groß- und Kleinschrift) und lassen Sie Ziffern und Satzzeichen an ihrem Platz, und schon haben Sie *IhiS2018dMg!* als Passwort.

Dieses Passwort errät niemand, der nicht Ihren speziellen Satz kennt. Sie selbst wiederum erinnern sich an diesen Satz sehr einfach und können das Passwort heruntertippen, während Sie ihn denken. Das unleserliche Passwort selbst brauchen Sie sich gar nicht merken.

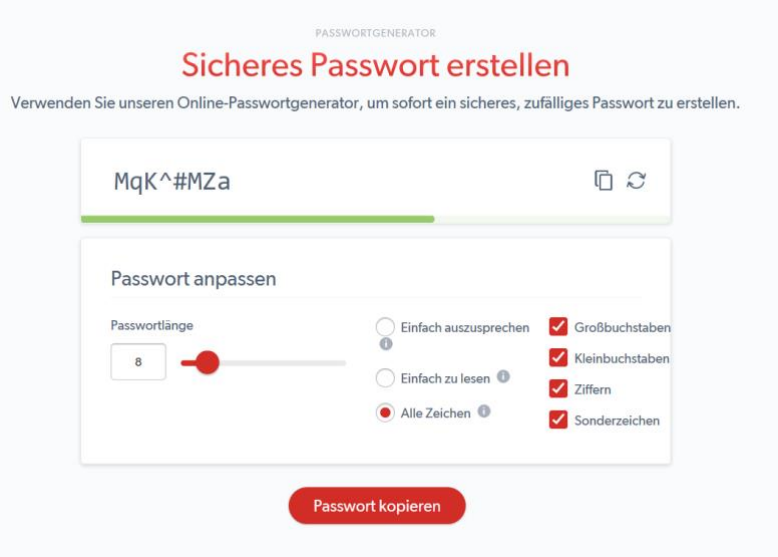
Verwendung eines Passwort-Generators

Eine weitere Alternative ist die Verwendung eines Passwort-Generators, also eines Programms bzw. einer Webseite, die Ihnen nach bestimmten Vorgaben sicher Passwörter generiert.

Kostenlos finden Sie dies beispielsweise unter https://www.lastpass.com/de/password-generator

Wählen Sie gewünschte **PASSWORTLÄNGE** ein, wählen Sie ob **GROßBUCHSTABEN**, **KLEINBUCHSTABEN**, **ZIFFERN** und/oder **SONDERZEICHEN** verwendet werden sollen. Auf Wunsch können Sie dann das Passwort noch für das Lesen oder Sprechen optimieren, diese Einstellungen beeinflussen die Verwendung von Sonderzeichen bzw. leicht verwechselbaren Zeichen im Passwort.

So geht’s leichter | Passwörter im Griff



Aus LastPass können Sie das Kennwort dann über das Symbol mit den beiden Seiten oben rechts in die **ZWISCHENABLAGE** kopieren und vor dort aus weiterverwenden.

Regelmäßiger Passwortwechsel: Pro und Contra

Große Erschütterung Anfang 2020: Das BSI, Herrscher über die Standard-Sicherheitsvorgaben in Deutschland, hat die Vorgaben für Passwörter geändert. Sind Passwörter also nicht mehr so wichtig? Können Sie darauf verzichten, diese sicher auszugestalten? Natürlich nicht. Das BSI hat nur einen kleinen Teil der Anforderungen verändert!

So geht’s leichter | Passwörter im Griff

Bisher war es so, dass im BSI-Grundschutzhandbuch unter anderem vorgeschrieben, dass ein Passwort regelmäßig geändert werden müsse. Auch die Länge und Komplexität der Passwörter war geregelt. Diese beiden Vorgaben standen aber schon lange in der Kritik der Experten.

Je mehr man einem Benutzer vorschreibt, dass er sein Passwort erneuern muss, und je komplexer man es verlangt, desto mehr steigt die Gefahr, dass dieser es sich irgendwo unsicher aufschreibt. Das hat am Ende viel schlimmere Auswirkungen als ein Passwort, dass weniger komplex ist oder länger nicht geändert wird.

Davon aber nicht betroffen sind die allgemeinen, eigentlich vollkommen logischen Anforderungen: Wenn Sie das Gefühl haben, dass jemand Ihr Passwort erraten hat oder en Konto kompromittiert wurde, dann ändern Sie natürlich das Passwort. Und auch wenn die Komplexität nicht extrem hoch sein soll, dann sollten Sie immer noch auf leicht zu erratende Zahlenkombinationen oder Worte verzichten. Diese sind und bleiben trotzdem unsicher!

Sichere Passwörter alleine helfen nicht

Ihre Passwörter sind von der Relevanz her wie ein Schlüssel. Nur die Personen, die Zugang benötigen, haben einen, und benutzen ihn auch. Lassen Sie den Schlüssel einfach mal so rumliegen?

Eher nicht, der ist am Schlüsselbund und der Schlüsselbund immer in Ihrer Nähe. Ähnlich verhält es sich mit Passwörtern. Ein gutes und sicheres Passwort alleine hilft Ihnen gar nichts, wenn Sie es nicht geheim halten. Und dazu zählt mehr, als es nicht laut auszusprechen!

So geht's leichter | Passwörter im Griff

Physische Aufbewahrung ist ungünstig

Wir Menschen sind manchmal noch sehr analog. Was wir uns merken wollen, das schreiben wir lieber mal auf. Man weiß ja nie, wann man die Information wieder braucht und wie es dann um die Erinnerung bestellt ist!

Das ist leider auch nicht selten bei Passwörtern der Fall. Viele der Vorfälle, bei denen Passwörter bekannt geworden sind oder Unbefugte mit gestohlenen Zugangsdaten in Rechner und Systeme eingebrochen sind, haben keine technischen Ursachen. Der Anwender ist das Problem.

Sie ändern das Passwort, das aber meist nicht in Ruhe, sondern „mal eben" zwischendurch.

Nur ist „mal eben" der kleine Bruder von „unkonzentriert". Sie schreiben das neue Passwort auf einen Klebezettel. Den packen Sie dann bevorzugt unter die Schreibtischunterlage.

Oder an die Rückseite des Monitors. Es gibt sogar Untersuchungen, dass diese Zettel immer an der jeweils anderen Seite Ihrer Schreibhand kleben. Weil Sie sich anstrengen müssen, einen solchen Zettel als Rechtshänder an der linken Seite des Monitors zu befestigen, kommt auch kein anderer Mensch darauf.

Unnötig zu sagen, dass diese Orte genau die sind, an denen Unholde als erstes nach einem Passwort suchen. Die elektronische, sichere und damit deutlich empfehlenswertere Version des Klebezettels ist der Passwort-Manager. Mehr dazu später!

So geht's leichter | Passwörter im Griff

Mein Passwort, nicht Dein Passwort

Passwörter sind etwas Persönliches. Aus vielen verschiedenen Gründen. Zum einen schon deshalb, weil nur über die Kombination aus Benutzername und Passwort nachweisbar ist, dass Sie eine bestimmte Dateneingabe oder -änderung, eine Transaktion oder Bestellung tatsächlich gemacht haben.

Wenn Sie Passwörter an andere Personen weitergeben, dann geben Sie gleichzeitig diese Sicherheit auf. Was immer diese Personen dann mit dem zugehörigen Benutzerkonto anstellen, es wird immer Ihnen angelastet werden. Das kann einigen Schaden verursachen.

Aus diesem Grund sollten Sie auch möglichst nicht im Büro Ihre Anmeldedaten weitergeben, wenn Sie in den Urlaub gehen. Auch wenn das gängige Praxis ist: Die charmantere Lösung ist die Einrichtung einer Vertreterrolle, wie Sie sowohl die Standard-Mailprogramme wie Outlook als auch alle Buchhaltungs- und Warenhaltungssysteme im Standard unterstützen. Damit kann der Vertreter dann auf Ihre Daten zugreifen, alle Änderungen werden aber in seinem Namen gemacht!

Natürlich spricht – wenn das Vertrauen da ist – nichts gehen das Teilen eines Amazon-Kontos innerhalb der Familie, damit alle Mitglieder darauf zugreifen können. Am Ende ist es immer eine Abwägung des Nutzens gegen das entstehende Risiko!

So geht's leichter | Passwörter im Griff

Besser kein Zusammenhang zur eigenen Person

Einfache Zahlen- und Ziffernfolgen sind keine gute Idee, das haben Sie mittlerweile schon häufiger gelesen und auch schon vorher selber so gesehen. Was im ersten Moment weniger einsichtig ist: Auch Ihnen bekannte Daten und Begriffe sind keine guten Passwörter.

Der BVB-Fan, der *BorussiaBVB09!* als Passwort wählt, hat zwar rein formal ein sicheres Passwort gewählt. Wenn Ihr Schreibtisch aber voll mit BVB-Devotionalien steht, dann ist auch das mit wenig Aufwand zu erraten.

Auch persönliche Daten wie Geburts- und Hochzeitstage, Namen von Haustieren und andere sind eher ungeeignet. Wenn Sie sich nur ein wenig in sozialen Netzwerken bewegen, dann sind diese Daten auf Ihren Posts oft ableitbar. Noch schlimmer: Facebook & Co. lieben Kettenbrief-Beiträge.

„Jetzt nehme ich das einfach mal auf: Otto Ottensen hat mich eingeladen, 12 Fragen über mich zu beantworten. Ich nominiere Petra Petersen, das auch zu machen."

Ganz zufällig sind diese 12 Fragen dann darauf ausgelegt genau solche Informationen über Sie zu erfragen. Was Facebook weiß, weiß die Welt. Abgesehen davon: Genau diese Informationen werden oft dazu verwendet, ein vergessenes Passwort wiederherstellen zu lassen beziehungsweise ein neues anzufordern: Viele Anbieter lassen Sie beim

So geht's leichter | Passwörter im Griff

Anlegen des Kontos genau solche Fragen beantworten und speichern die Antworten. Wer diese Antworten kennt, der kann leichter auf Ihre Daten zugreifen!

Passwörter sind keine Highlander

„Es kann nur einen geben" mag im Filmklassiker Highlander seine Berechtigung gehabt haben, bei Passwörtern definitiv nicht. Es hilft Ihnen wenig, wenn Sie sich ein supertolles, komplexes und trotzdem für Sie einfach zu merkendes Passwort ausdenken und es dann überall verwenden. Bei Amazon, eBay, Ihrer Bank, dem Forum für Autofans und dem kleinen, windigen Laden in einem Randgebiet der Welt.

Je mehr Dienste und Seiten Sie mit denselben Zugangsdaten nutzen, desto mehr potenzielle Angriffspunkte bieten Sie. Es kommt immer wieder vor, dass durch eine Datenlücke Benutzernamen und Passwörter abfließen. Diese Informationen finden sich dann in Datenbanken im Internet, die der interessierte Cyberkriminelle günstig erwerben kann. Und der setzt genau auf die Erfahrung, dass viele Anwender dieselbe Kombination aus Benutzernamen und Passwort auf mehreren Seiten nutzen. Nichts liegt also näher, als diese Kombination einfach mal auf diversen Seiten auszuprobieren.

So geht's leichter | Passwörter im Griff

Hinzu kommt, dass Sie im Falle eines Datenlecks das Passwort schnell ändern müssen. Wenn Sie wissen, welches Konto oder welcher Dienst betroffen war, dann fällt das nicht gar so schwer. Sie rufen die Seite auf, melden sich an, klicken auf **Passwort ändern** und vergeben ein neues.

Verwenden Sie immer die gleiche Kombination, dann ist es eben nicht nur eine Seite, auf der Sie die Zugangsdaten ändern müssen, sondern eine Vielzahl. Im schlimmsten Fall wissen Sie nicht mal mehr, wo Sie die kompromittierten Zugangsdaten überall verwendet haben und können Sie nicht überall ändern.

Vermeiden Sie Muster

Die meisten Menschen denken strukturiert und entwickeln Systeme, auch bei Passwörtern. Das ist auf den ersten Blick eine gute Idee, trägt es doch zur besseren Merkbarkeit bei. Genauer betrachtet aber machen Sie damit ein eigentlich gutes Passwort schnell zunichte.

Das aus dem Satz „Ich habe im Sommer 2018 den Motorradführerschein gemacht!" abgeleitete Passwort *IhiS2018dMg!* ist super. Wenn Sie als nächstes dann aber einfach die Jahreszahl ändern, wenn Sie zur Änderung des Passwortes aufgefordert werden, dann nimmt die Sicherheit rapide ab.

Bei gestohlenen Passwörtern werden automatisch auch „Weiterentwicklungen" ausprobiert. *IhiS20**19**dMg!* und *IhiS20**20**dMg!* sind da auch für den einfachsten Cyberkriminellen allzu naheliegend.

Dasselbe trifft dann auch Passwörter wie *Passwort2005!*, Kombinationen aus einem festen Text und wechselnden Jahres- und Monatsziffern. Auch wenn diese einmal mehr bei einem Passwortcheck als gut (weil aus Klein- und Großbuchstaben, Ziffern, Sonderzeichen bestehend) bewertet werden würden.

So geht’s leichter | Passwörter im Griff

Die Quintessenz: Das für sie beste Passwort ist immer eine Kombination aus vielen Faktoren: Technische Anforderungen, persönliche Präferenzen und das menschliche Auge für alle nicht technisch zu erkennenden Schwächen müssen hier zusammenspielen.

Über Ihre Schulter

Die Eingabe von Passwörtern sollte immer so erfolgen, dass niemand anderes das Passwort ablesen kann. Das wird vom System unterstützt, indem es nicht die Zeichen des Passwortes anzeigt, sondern nur Sternchen.

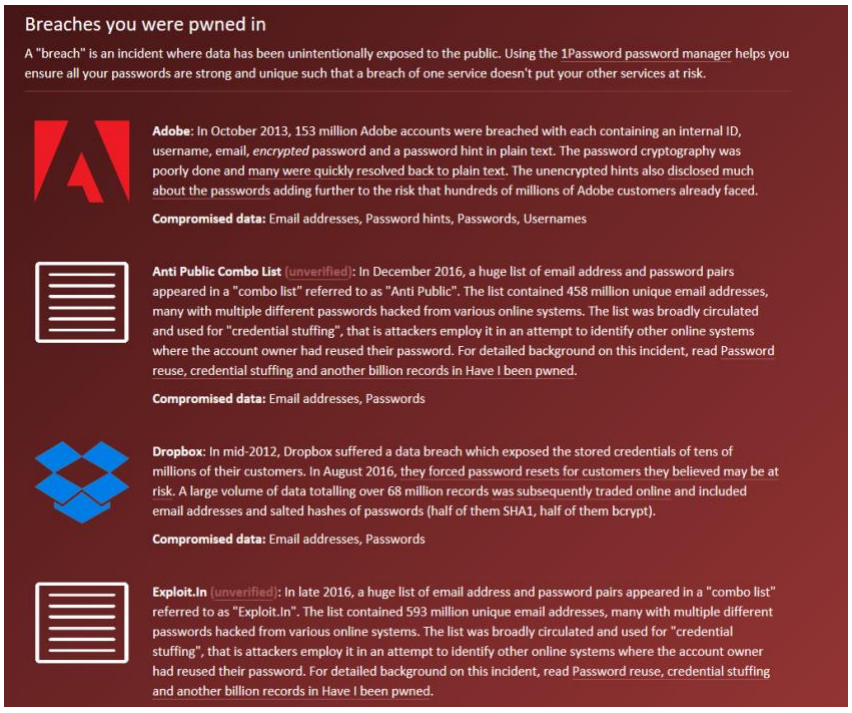
Nutzen Sie in der Öffentlichkeit am besten nicht die Möglichkeit, sich durch einen Klick auf das Symbol mit dem Auge das eingegebene Passwort anzeigen zu lassen. Achten Sie ebenfalls darauf, dass niemand auf Ihre Tastatur schauen kann und das Passwort mitlesen kann.

Das geht mit geübtem Auge recht schnell. Dazu kommt, dass an öffentlichen Orten oft Web- oder Sicherheitskameras aufgehängt sind. Aus den Aufzeichnungen kann das Kennwort bei der Eingabe auf der Tastatur problemlos abgelesen werden, wenn die Kamera (un)günstig ausgerichtet ist.

So geht’s leichter | Passwörter im Griff

Ist es schon zu spät?

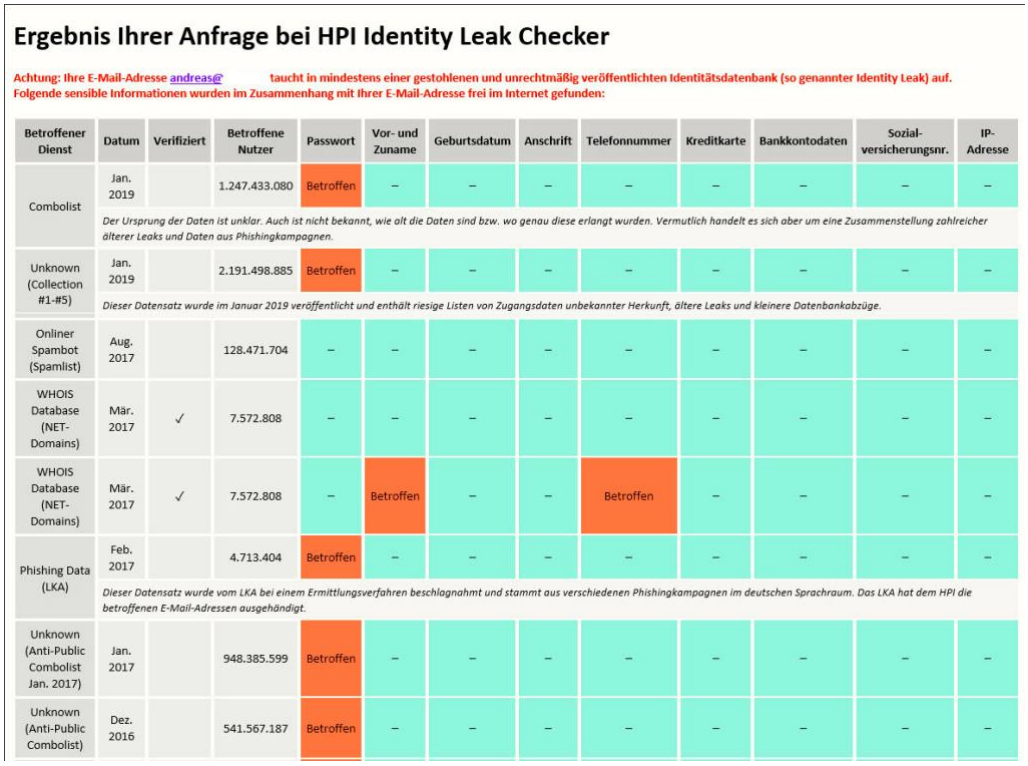
Immer wieder kommen Datenlecks und -pannen in die Nachrichten: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen und im Internet verkauft. Der Käufer hat dann so lange theoretisch Zugriff auf all Ihre Benutzerkonten, wie Sie das Passwort nicht geändert haben.



Die bekanntesten Sicherheitsvorfälle (zumindest die, die bekannt geworden sind), sind auf der Seite https://haveibeenpwned.com/ zusammengefasst. Dort können Sie nach Eingabe Ihres Passwortes sehen, ob und bei welchem Hack Ihre Zugangsdaten erbeutet wurden.

So geht’s leichter | Passwörter im Griff

Auch das Hasso-Plattner-Institut bietet mit dem kostenlosen Identity Leak Checker unter https://sec.hpi.de/ilc/ einen entsprechenden Service.



Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse andreas@ taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
Combolist	Jan. 2019		1.247.433.080	Betroffen	–	–	–	–	–	–	–	–
	Der Ursprung der Daten ist unklar. Auch ist nicht bekannt, wie alt die Daten sind bzw. wo genau diese erlangt wurden. Vermutlich handelt es sich aber um eine Zusammenstellung zahlreicher älterer Leaks und Daten aus Phishingkampagnen.											
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–	–	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.											
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–	–
WHOIS Database (NET-Domains)	Mär. 2017	✓	7.572.808	–	–	–	–	–	–	–	–	–
WHOIS Database (NET-Domains)	Mär. 2017	✓	7.572.808	–	Betroffen	–	–	Betroffen	–	–	–	–
Phishing Data (LKA)	Feb. 2017		4.713.404	Betroffen	–	–	–	–	–	–	–	–
	Dieser Datensatz wurde vom LKA bei einem Ermittlungsverfahren beschlagnahmt und stammt aus verschiedenen Phishingkampagnen im deutschen Sprachraum. Das LKA hat dem HPI die betroffenen E-Mail-Adressen ausgehändigt.											
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948.385.599	Betroffen	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–	–	–	–

Geben Sie auf der Seite die E-Mail-Adresse ein, und Sie bekommen an genau diese E-Mail-Adresse eine Liste der Leaks, in denen sie sich befindet. In dieser E-Mail finden Sie noch detailliertere Informationen als in der Datenbank von HaveIBeenPwned: Sie sehen nicht nur, ob die Adresse betroffen war, sondern auch, welche Daten abgeflossen sind.

Wenn Sie betroffen sind, dann ändern Sie so schnell wie möglich das Passwort, und wiederholen Sie dies häufiger. Auch wenn Sie das nach dem Vorfall wissentlich oder unwissentlich schon gemacht haben: Besitzer der erbeuteten Daten wissen zumindest, dass die Benutzernamen und E-Mail-Adressen existieren und müssen sich so nur noch darauf konzentrieren, das Passwort herauszufinden.

So geht’s leichter | Passwörter im Griff

Keine dieser Datenbanken erhebt natürlich Anspruch auf Vollständigkeit. Nur, weil Ihre E-Mailadresse nicht als betroffen gekennzeichnet wird, können damit zusammenhängende Kombinationen aus Benutzername und Kennwort trotzdem in die falschen Hände gelangt sein!

Echten Schutz dagegen gibt es nicht. Natürlich macht es Sinn, Ihre Kennwörter auch ohne konkreten Anlass regelmäßig zu ändern, und dabei eben keine erkennbare Systematik zu verwenden. Ab dem Zeitpunkt der Änderung ist der Zugang für einen Fremden mit den erbeuteten Passwörtern nicht mehr möglich.

Vorsicht vor Phishing

Phishing an sich ist schon gemein, weil es dem Anwender durch Vorgaukeln einer echten Anfrage eines Dienstanbieters (wie PayPal, Amazon etc.) die Zugangsdaten aus der Tasche ziehen will. Nur sind die Anwender mittlerweile nicht mehr ganz so blauäugig und erkennen die gefälschten Mails oft schon.

Daher gibt es eine neuere, noch fiesere Variante: Aus den im Internet verfügbaren Datenbankenmit E-Mail-Adressen und Passwörtern werden Serien-E-Mails generiert. Diese sagen grob, dass Ihr Konto geknackt wurde, als Beweis wird Ihnen das Passwort in Klarschrift mitgeteilt.

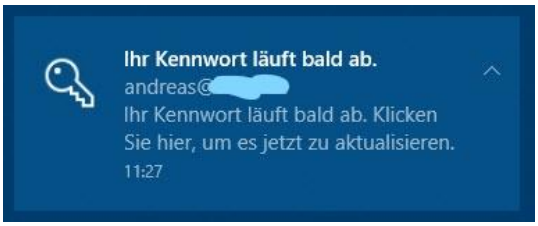
Komfortabel enthält die E-Mail dann einen Link, mit dem Sie schnell das Passwort für das Konto ändern können. Dieser führt dann wie bei Phishing-Mails üblich auf eine gefälschte Seite, auf der dann weiter Daten gestohlen werden.

Das Perfide daran: Dadurch, dass Sie ein echtes, von Ihnen verwendetes Passwort in der Mail angezeigt bekommen, denken Sie weniger über die Echtheit der Mail nach und klicken schneller auf den Link.

So geht's leichter | Passwörter im Griff

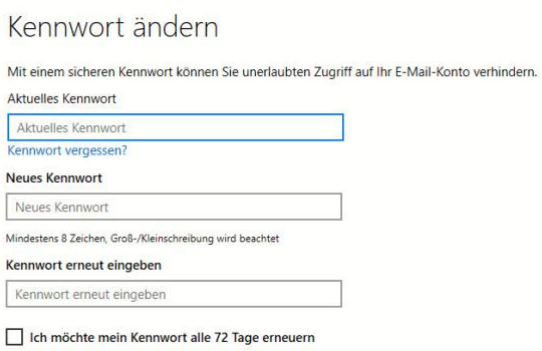
Automatischen Kennwortwechsel ausschalten

Sie sitzen an Ihrem Windows 10-PC, denken an nichts Böses, und schon poppt eine Meldung hoch, dass Ihr Kennwort in wenigen Tagen abläuft und Sie dieses Ändern sollen. Regelmäßige Kennwortwechsel machen durchaus Sinn, allerdings zeigen die oben zitierten Analysen des BSI, dass das auch kontraproduktiv sein kann. Sie haben unter Windows 10 die Freiheit, das für sich einzustellen.



Die Systemmeldung "Ihr Kennwort läuft bald ab. Klicken Sie hier, um es jetzt zu aktualisieren" kommt immer dann, wenn Sie in den Kontoeinstellungen aktiviert haben, dass Sie alle 72 Tage einen Wechsel des Kennworts erzwingen wollen. Dann haben Sie für das aktuelle Passwort keine andere Chance, als eine Änderung vorzunehmen.

Klicken Sie auf den Meldungstext, dann werden Sie auf die Kontoseite Ihres Microsoft-Kontos im Internet geleitet. Zum Ändern des Kennwortes geben Sie das aktuelle, dann zweimal identisch das neue Kennwort ein. Stellen Sie dann sicher, dass die Checkbox **Ich möchte mein Kennwort alle 72 Tage erneuern** deaktiviert ist.



Ist diese aktiviert, dann hält Microsoft die Zeit, die nach der letzten Änderung des Kennwortes vergangen ist, nach. Nach 72 Tagen fordert Sie Windows dann mit der obigen Meldung zur Änderung des Kennwortes auf.

So geht’s leichter | Passwörter im Griff

Externe Expertise: Der Google-Sicherheitscheck

An den Diensten von Google kommen Sie kaum noch vorbei. Wenn Sie ein Smartphone mit Android als Betriebssystem haben, dann nutzen Sie den Play Store, GMail, das Google Drive und andere Services. Aber auch bei einer normalen Websuche läuft Ihr Google-Konto im Hintergrund mit, um Daten zu sammeln und Sie damit zu unterstützen. Kurz: Google kennt eine Menge Daten von Ihnen. Führen Sie regelmäßig den Google-Sicherheitscheck durch, um Risiken zu minimieren!

Wir haben Ihre gespeicherten Passwörter analysiert und die folgenden Probleme gefunden

Beim Sicherheitscheck erhalten Sie personalisierte Sicherheitsempfehlungen für Ihr Google-Konto. Jetzt starten

Nach Aufruf der Seite und Anmeldung mit Ihren Google-Kontodaten zeigt Ihnen der Sicherheitscheck die gefundenen Sicherheitsrisiken an. Keine Sorge: Nicht alle sind wirklich gefährlich, sollten aber einzeln betrachtet werden.

Unter **Meine Geräte** zeigt Google alle Geräte an, die schon länger nicht mehr mit den Google-Diensten verbunden waren. Das passiert vor allem

So geht's leichter | Passwörter im Griff

dann, wenn Sie ein Gerät verkauft haben. Da Sie das sicherlich gelöscht haben, kann damit nichts mehr passieren. Trotzdem: Löschen Sie nicht mehr vorhandene Geräte aus Ihrem Google-Konto!

Ganz unten finden Sie den Passwortcheck. Führen Sie diesen nach erneuter Anmeldung aus, dann zeigt Ihnen Google eine Bewertung alles Passwörter an, die in Ihrem Google Account gespeichert sind. Das ist natürlich nur ein Bruchteil all Ihrer verwendeten Passwörter, zeigt aber gegebenenfalls schon einmal Schwächen, die Sie auch bei anderen Konten in Kauf nehmen.

Passwörter im Browser

Wenn sie einmal Ihre Passwörter durchforsten, dann fällt eines schnell auf: Abgesehen von den Zugangsdaten zu Ihren Geräten gehören die fast alle zu einem Online-Dienst. Selbst früher so analoge Dinge wie der Kontakt zu einer Versicherung sind mittlerweile auf Online-Portale umgestellt. Die Folge: zum Zugriff auf fast alle Dienste verwenden Sie

So geht's leichter | Passwörter im Griff

den Webbrowser. Damit ist der zentrales Instrument und wenig verwunderlich mittlerweile auch schon im Standard gut gerüstet. Alle aktuellen Webbrowser unterstützen Sie bei der Verwendung und Eingabe von Passwörtern.

Der Browser hat bei den Programmen in Windows (und auch macOS) eine Sonderstellung: Auf Grund der Natur der Daten, die er verarbeitet, hat er per se hohe Sicherheitsanforderungen. Verschlüsselte Webseiten, Zugänge zu kritischen Systemen wie dem Online-Banking, Kundenkonten von Online-Apotheken und Händlern, alleine die Datenübertragung beinhaltet so viele potenziell schützenswerte Daten, dass die Browser voller Technik zu deren Schutz sind.

Chrome beispielsweise bietet zusätzlich eine eigene Erweiterung an, die die Verwaltung von Passwörtern nochmal komfortabler macht.

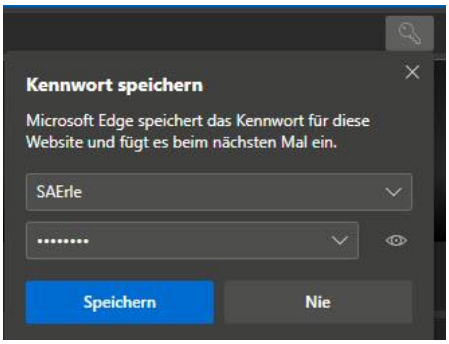
Zu guter Letzt bieten die Browser die Synchronisation von Passwörtern zwischen den Geräten an, gespeicherte Passwörter sind damit auch auf dem Smartphone oder Tablet verfügbar, wenn Sie auf allen Geräten denselben Browser verwenden (und sich mit einem Konto in den Browsern anmelden und die Synchronisierung aktiviert haben).

Der Umgang mit Passwörtern in Edge

Die folgenden Beschreibungen beziehen sich auf die neue Version von Edge („Edge Chromium"). Sollten Sie diese noch nicht im Rahmen eines Updates oder manuell installiert haben, dann holen Sie dies unter https://www.microsoft.com/edge?form=MA13DE&OCID=MA13DE nach. Ab der Windows-Version 2004 solle er automatisch verfügbar sein.

So geht's leichter | Passwörter im Griff

Automatische Speicherung von Passwörtern

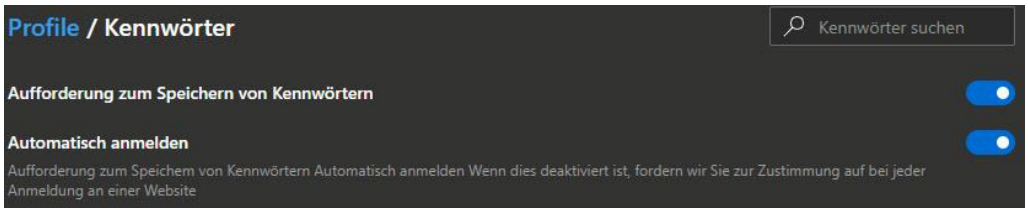


Im Standard speichert Edge die Passwörter auf Nachfrage. Die Kombination von Webseite, Benutzername und Passwort wird in einer internen. Verschlüsselten Datenbank abgelegt und bei jeder neuen Anmeldung auf dieser Seite wieder vorgeschlagen.

Sie können sich das eingegebene Passwort anzeigen lassen ,indem Sie auf das Auge neben dem durch Sterne maskierte Passwort klicken. Wenn Sie die Speicherung im Einzelfall nicht wünschen, dann klicken sie auf **Nie**. Das verhindert auch die Nachfrage bei weiteren Anmeldungen auf der entsprechenden Webseite.

Wenn Sie die automatische Speicherung der Passwörter ausschalten wollen – beispielsweise, weil es sich um einen von mehreren Personen genutzten PC handelt – dann bedarf dies nur weniger Schritte.

Klicken Sie in Edge auf die drei Punkte oben rechts, dann auf **Einstellungen** > **Profile** > **Kennwörter**.



Unter **Aufforderung zum Speichern von Kennwörtern** können Sie die automatische Speicherung deaktivieren. Wenn Sie die Passwörter gespeichert haben möchten, aber diese nicht automatisch zu Anmeldung herangezogen werden sollen, dann deaktivieren Sie den Schalter neben **Automatisch anmelden**.

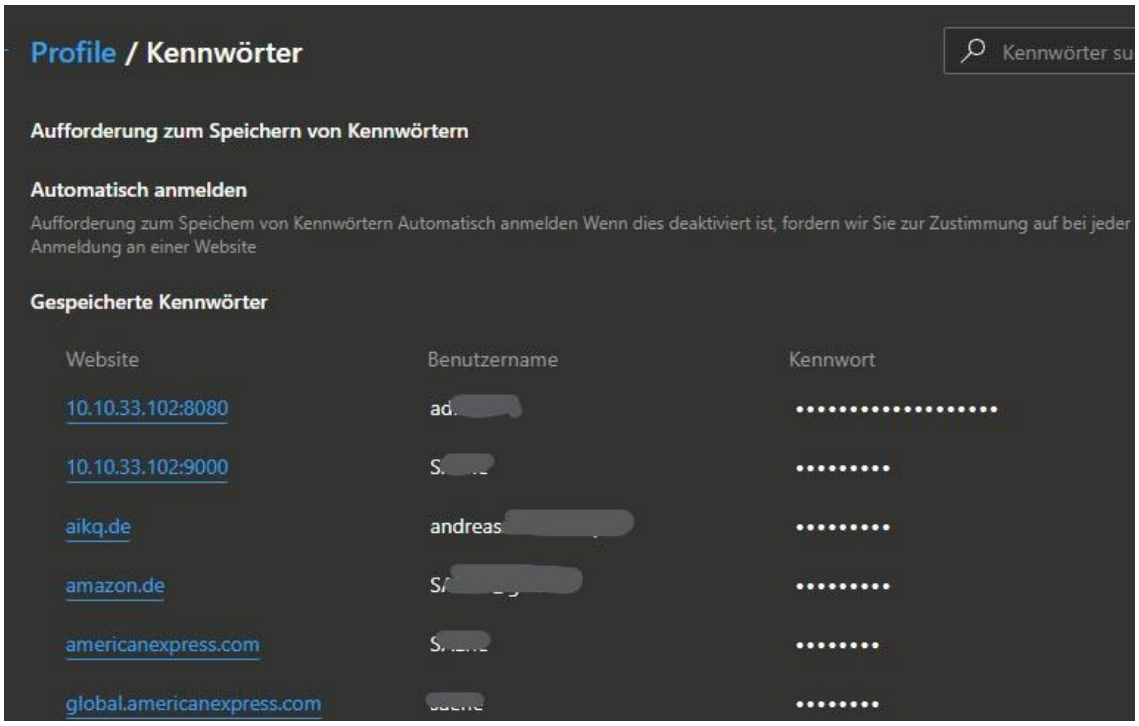
So geht's leichter | Passwörter im Griff

Exportieren und Nachsehen der Passwörter in Edge

Es gibt eine Vielzahl von Webseiten, auf denen Sie sich anmelden müssen. Wenn Sie den Schutz so stark wie eben möglich haben wollen, dann verwenden Sie unterschiedliche Kombinationen für die Anwendung. Das hat den Nachteil, dass Sie sich viele Informationen merken müssen. Edge bietet hier eine tolle, aber auch mit Vorsicht zu genießende Hilfe.

Sie kennen die Situation bestimmt: Da Gehirn ist noch wach, das Gedächtnis gut und so können Sie sich alle Kombinationen von Benutzernamen und Kennwort merken.

Bis Sie dann eine Seite länger nicht mehr besucht haben und in der Folge genau deren Zugangsdaten vergessen haben. Wenn Sie keinen Passwort-Manager verwendet haben, dann ist guter Rat teuer. Es sei denn, Sie verwenden einen versteckten Kniff in Edge. Der erlaubt nämlich den Export der darin gespeicherten Passwörter.



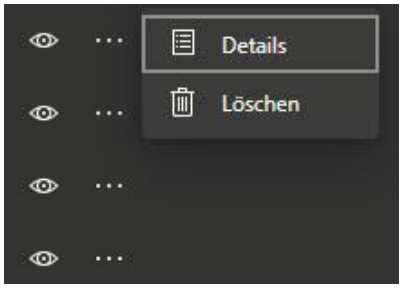
So geht's leichter | Passwörter im Griff

Klicken Sie auf die drei Punkte oben rechts am Bildschirm, dann auf **Einstellungen** > **Profile** > **Kennwörter** zeigt Edge Ihnen alle Webseiten an, auf denen Sie ein Passwort gespeichert haben. Ein Klick auf das Augen-Symbol rechts von einem Eintrag ändert die angezeigten Sternchen dann in das gespeicherte Passwort.

Um alle Passwörter in einer Excel-Tabelle zu erhalten, klicken Sie auf die drei Punkte neben **Gespeicherte Kennwörter** und wählen Sie dann **Kennwörter exportieren**. Vorsicht: Diese Excel-Tabelle in den Händen eines Unbefugten verursacht größtmöglichen Schaden: Darin stehen die Webseiten-URLs und die Kennwörter in Klarschrift!

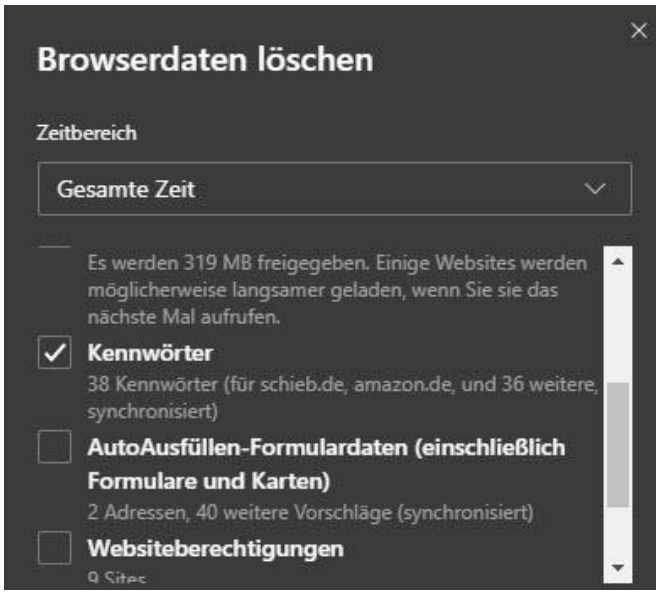
Löschen der Passwörter in Edge

Mit der Zeit werden Sie eine Vielzahl von Kennwörtern im Browser gespeichert haben. Manche davon werden veralten, andere wollen sie vielleicht aus Sicherheitsgründen manuell löschen. Das lässt sich in Edge auf zwei Arten erreichen:



Wenn Sie nur ein einzelnes Paar aus Benutzernamen und Kennwort löschen wollen, dann klicken Sie auf die drei Punkte oben rechts am Bildschirm, dann auf **Einstellungen** > **Profile** > **Kennwörter** zeigt Edge Ihnen alle Webseiten an, auf denen Sie ein Passwort gespeichert haben. Klicken Sie auf die drei Punkte neben der URL der Webseite, dann auf **Löschen**. Nur dieser Eintrag wird damit gelöscht.

So geht's leichter | Passwörter im Griff



Um alle gespeicherten Kennwörter zu löschen, klicken Sie in den Einstellungen von Edge auf **Datenschutz und Dienste** > **zu löschende Elemente auswählen**. Wählen Sie unter **Zeitbereich** die Option **Gesamte Zeit**. Deaktivieren Sie dann alle Optionen in der Liste bis auf Kennwörter. Der Klick auf **Jetzt löschen** entfernt alle Kennwörter aus Edge.

Synchronisieren der Passwörter in Edge

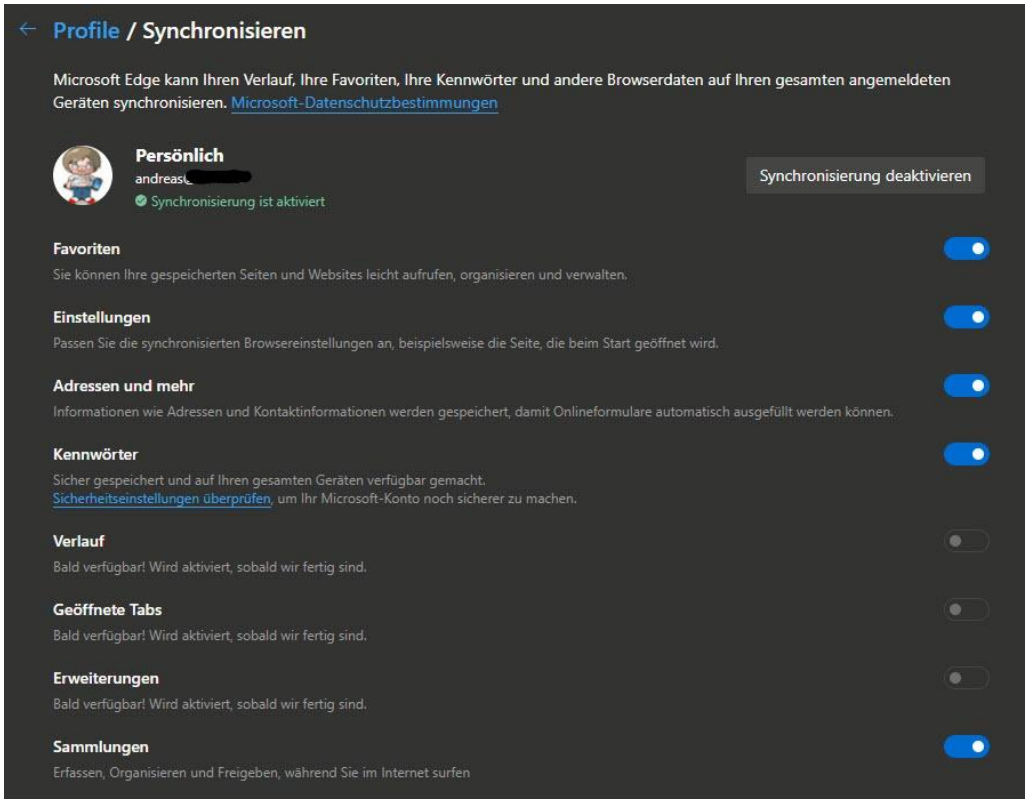
In der Praxis verwenden Sie meist mehrere Geräte, mit denen Sie auf das Internet zugreifen und damit auch die Anmeldungen an Webseiten und Diensten durchführen. Wenn die meisten Browser haben einen eigenen zugehörigen Dienst (Microsoft das Microsoft-Konto, Google den Google-Account etc.).

Darüber können Sie die Kennwörter dann synchronisieren. Wenn Sie dann denselben Browser auf einem anderen Endgerät nutzen und dort ebenfalls die Synchronisation eingeschaltet haben, sind Sie immer synchron. Die bisher gespeicherten Passwörter sind verfügbar und neu hinzugefügte oder veränderte Passwörter werden auf die anderen Geräte übertragen.

Um die Synchronisation in Edge zu aktivieren, klicken Sie auf das Symbol mit dem Kopf oben rechts in Edge und dann auf **Anmelden**.

So geht's leichter | Passwörter im Griff

Geben Sie die Zugangsdaten Ihres Microsoft-Kontos ein und bestätigen Sie die Anmeldung.



Wenn Sie dann auf **Einstellungen** > **Profile** > **Synchronisierung** klicken, können Sie ganz fein einrichten, welche Elemente mit der Cloud synchronisiert werden sollen. Darunter eben auch die Passwörter.

Hier hat der neue Edge-Browser im Gegensatz zu seinen Vorgängern den Vorteil, dass er auch auf dem Mac verfügbar ist und sogar für Linux angekündigt wurde. Somit können Sie ihn auf allen gängigen Systemen benutzen.

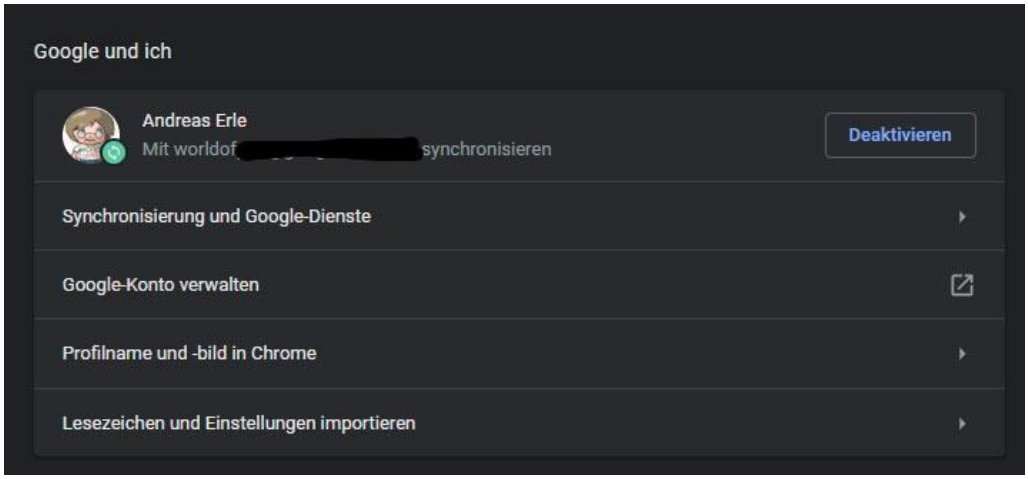
Passwortverwaltung in Google Chrome

Natürlich bieten auch die anderen Browser die Möglichkeit, Kennwörter zu speichern und diese zu synchronisieren. Google Chrome

So geht's leichter | Passwörter im Griff

beispielsweise verhält sich hier sehr ähnlich wie der neue Edge. Wenig verwunderlich, schließlich basieren beide Browser auf Chromium und haben damit sehr viele gleiche Elemente.

Bei Chrome melden Sie sich statt mit dem Microsoft-Konto natürlich mit Ihrem Google-Account an. Klicken Sie dazu auf **Einstellungen** > **Google und ich** klicken auf **Anmelden**. Geben Sie die Zugangsdaten Ihres Google-Accounts ein und bestätigen Sie die Anmeldung. Auf dem selben Weg können Sie dann über Deaktivieren die Synchronisation wieder ausschalten.



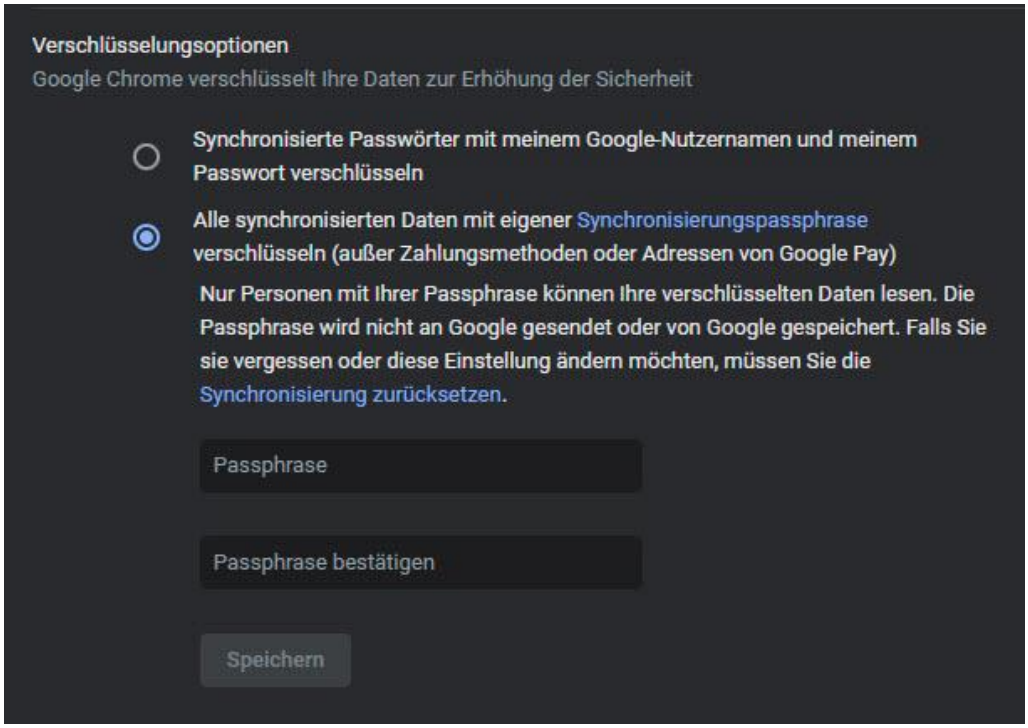
Unter auf **Einstellungen** > **Google und ich** > **Synchronisierung verwalten** können Sie die einzelnen Synchronisierungsobjekte festlegen und die Passwörter explizit aktivieren oder deaktivieren.

Chrome bietet für die Passwörter noch eine weitere Schutzstufe: Wenn Sie unter **Google und ich** ein wenig nach unten Scrollen, dann können Sie die Option **Synchronisierte Passwörter mit meinem Google-Nutzernamen und meinem Passwort verschlüsseln** aktivieren.

Sollte also jemand auf die auf den Google-Servern abgelegte Synchronisationsdatei für die Passwörter kommen, dann kann er die nur mit Kenntnis Ihres Nutzernamens und des zugehörigen Passworts lesen.

So geht's leichter | Passwörter im Griff

Und wenn Ihnen das immer noch nicht reicht, dann können Sie eine eigene Passphrase angeben. Die wird dann verwendet, um alle synchronisierten Daten zu verschlüsseln und sie wird nicht an Google gesendet. Damit haben Sie ganz alleine den Zugriff auf die Passwörter (und andere synchronisierte Elemente).



Das Löschen und Exportieren von Passwörtern in Chrome funktioniert genauso wie für den neuen Edge-Browser oben beschrieben. Die Einstellungen finden Sie unter **Einstellungen** > **Autofill** > **Passwörter**.

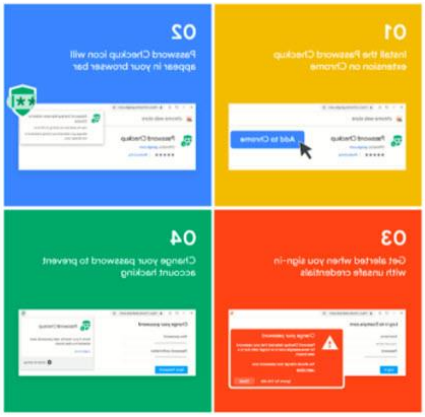
Dort können Sie auch deaktivieren, dass die Speicherung der Passwörter automatisch angeboten wird.

Passwort-Erweiterung Chrome

Kompromittierte Passwörter sind die Wurzel alles Übels: In den diversen Datenbanken im Internet, die Benutzernamen und Passwörter enthalten, können sich übelmeinende Genossen bedienen und sich an fremden

So geht's leichter | Passwörter im Griff

Konten anmelden. Sind Sie davon betroffen, dann kann das schlimme Auswirkungen haben,. Wenn Sie Google Chrome als Browser benutzen, dann können Sie sich die manuelle Prüfung sparen, ob Ihr Account betroffen ist!



Laden Sie sich die Erweiterung für Chrome kostenlos hier herunter. Wenn diese installiert ist, dann zeigt Ihnen Chrome ein grünes Symbol an. sobald Sie einen Benutzernamen und ein Kennwort eingeben, prüft die Erweiterung, ob der Account von einem der Google bekannten Datenlecks betroffen war und warnt automatisch durch ein deutlich sichtbares, rotes Hinweisfeld.

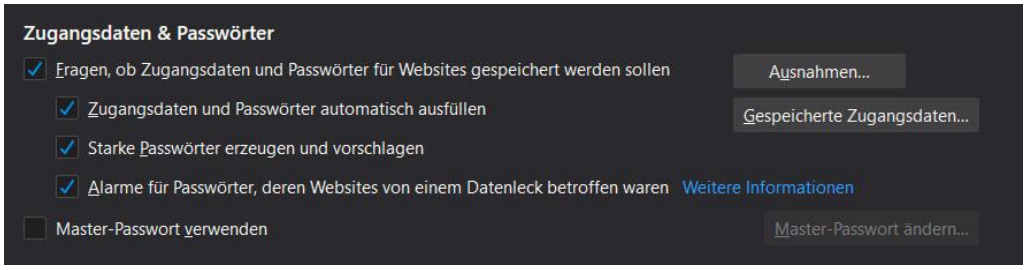
Dabei setzt Google nach eigenen Angaben Techniken ein, die die sensitiven Daten wie Benutzername und Kennwort schützen und gar nicht in die Hände von Google geben. Auf jeden Fall ein Schritt weiter in Richtung der automatischen Information der Benutzer, wenn sie potenziell von einem Sicherheitsleck betroffen sind!

Mozilla Firefox und die Passwörter

Auch Firefox hat eine integrierte Passwortverwaltung. Im Standard bietet Ihnen der Mozilla-Browser wie seine Konkurrenz an, die Passwörter zu speichern. Das können Sie ausschalten, wenn Sie es nicht wollen. Dazu klicken Sie auf die drei parallelen Striche am oberen, rechten Bildschirmrand, dann auf **Zugangsdaten und Passwörter**. Klicken Sie dann auf die drei Punkte am oberen, rechten Bildschirmrand, auf **Einstellungen** > **Datenschutz und Sicherheit** und aktivieren unter

So geht’s leichter | Passwörter im Griff

Zugangsdaten & Passwörter die Option **Fragen, ob Zugangsdaten und Passwörter für Website gespeichert werden sollen**.



Hier können Sie noch ein wenig mehr konfigurieren als bei den anderen Browsern. Beispielsweise können Sie Passwörter allgemein speichern lassen, durch einen Klick auf **Ausnahmen** aber festlegen, für welche Seiten das nicht der Fall sein soll.

Das kann als zusätzliche Sicherheitsschicht für besonders sensible Webseiten wie Online-Banking oder Versicherungen sinnvoll sein. Für diese Seiten müssen Sie dann das Passwort immer wieder manuell eingeben.

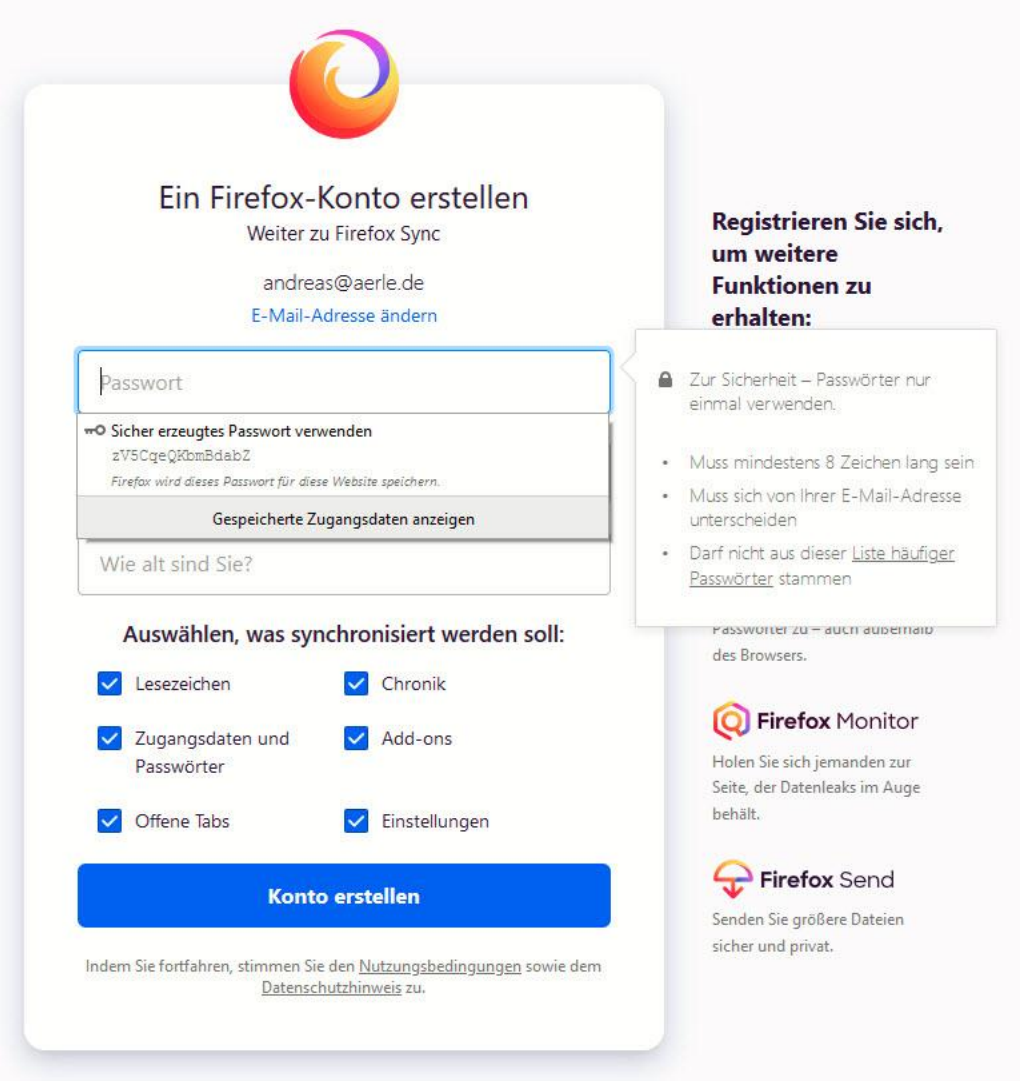
Eine weitere tolle Funktion ist die Warnung vor kompromittierten Passwörtern. Das können Sie unter **Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren** aktivieren.

Wenn Sie von Firefox gespeicherte Passwörter löschen wollen, dann geht das über die drei Punkte am oberen, rechten Bildschirmrand, auf **Einstellungen** >**Datenschutz und Sicherheit** > **Zugangsdaten & Passwörter** > **Gespeicherte Zugangsdaten** auf die Liste der Webseiten gehen und dann die gewünschten Zugangsdaten durch einen Klick auf den Papierkorb löschen.

So geht's leichter | Passwörter im Griff

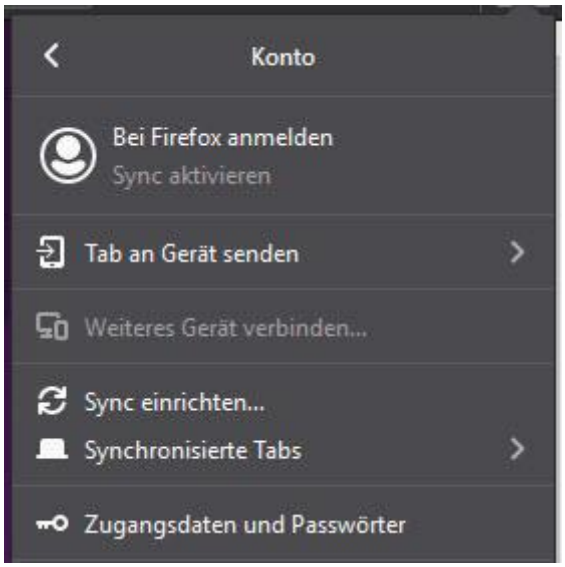
Firefox Lockwise – Synchronisation mit Mobilgeräten

Auch Firefox bietet einen geräteübergreifenden Sync an. Dazu müssen Sie sich allerdings ein – nicht ganz so übliches – Firefox Sync-Konto anlegen. Das geht kostenlos unter https://accounts.firefox.com/.



Schon im Anlegen dieses Kontos können Sie eingeben, welche Elemente aus Firefox Sie synchronisieren wollen. Dazu gehören natürlich auch die **Zugangsdaten und Passwörter**.

So geht's leichter | Passwörter im Griff



Wenn Sie bereits ein Konto bei Mozilla haben oder Ihre Synchronisationseinstellungen ändern wollen, dann klicken Sie auf den kleinen Kreis mit der Figur oben rechts im Firefox-Fenster und dann auf **Bei Firefox anmelden**. Über die Option Sync einrichten können Sie dann genau festlegen, welche Daten mit dem Konto synchronisiert werden. Natürlich inklusive der Passwörter!

Auf mobilen Geräten bietet Firefox Lockwise noch einen weiteren Vorteil: Separat von der mobilen Version des Firefox-Browsers lässt sich die Lockwise-App kostenlos auf iOS- und Android-Geräten installieren und gibt Ihnen Zugriff auf Ihre in Firefox gespeicherten und synchronisierten Passwörter. Das funktioniert sogar in beide Richtungen: In der App können Sie auch Passwörter eingeben, die dann nach der Synchronisation in Firefox auf allen Geräten zur Verfügung stehen!

Synchronisation von Passwörtern auf dem Mac

Wenn Sie nicht nur ein iPhone oder ein iPad, sondern auch einen Mac oder ein MacBook nutzen, dann ist der Schlüsselbund ein unverzichtbares Hilfsmittel. Wie sein Gegenstück im echten Leben hilft er Ihnen, Ihre Passwörter zwischen den Geräten zu synchronisieren und nicht mehr erneut eingeben zu müssen.

So geht's leichter | Passwörter im Griff

Der technische Kniff dabei ist die Nutzung von iCloud als Apples Cloud-Service, über den die Passwörter dann verschlüsselt und vor Fremdzugriff gesichert abgelegt werden. Jedes Gerät mit macOS oder iOS kann dann bei aktiviertem iCloud-Zugriff kann dann darauf zugreifen. Wichtig: Das funktioniert nur dann, wenn Sie auf allen Geräten dieselbe Apple ID nutzen!

Auf dem Mac muss der Schlüsselbund unter **Einstellungen** > **iCloud** eingeschaltet werden.

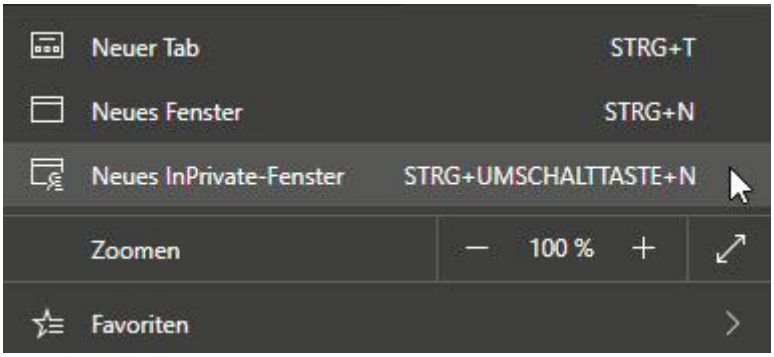
Auch mal ohne Passwörter: Der private Modus

Wenn Sie Ihren eigenen PC verwenden, dann haben Sie die Speicherung von eingegebenen Zugangsdaten unter Kontrolle. Anders verhält es sich, wenn Sie ein fremdes Gerät benutzen. Beim Freund um die Ecke, im Internetcafé im Urlaub, auf einem Arbeits-PC. Teilweise können Sie dort nicht einmal die Einstellungen verändern, wenig Chancen also, Ihre Passwörter zu schützen. Für solche Situationen bietet jeder Browser

So geht's leichter | Passwörter im Griff

einen privaten Surfmodus, in dem keine Daten gespeichert werden. Dazu gehören auch die eingegebenen Passwörter.

Eine private Surfsitzung aktivieren Sie immer im Browser selbst.



Bei Edge klicken Sie dazu auf die drei Punkte oben rechts, dann auf **Neues InPrivate-Fenster**. Bei Chrome finden Sie die Funktion an der selben Stelle, nur heißt sie da **Neues Inkognito-Fenster**, Bei Firefox schließlich **Neues privates Fenster**. Andere Browser haben diese Funktion an ähnlicher Stelle natürlich auch.

Zusätzliche Sicherheit 2FA und Token

Mit Netz und doppeltem Boden, das ist die klassische Absicherung in vielen Bereichen des täglichen Lebens. Eine alleineige Kombination aus Benutzername und Passwort ist anfällig: Kommt ein Fremder in deren Besitz, weil er Sie aus einem Datenleck bekommen, von Ihren Fingern abgelesen oder erraten hat, dann kommt er ohne weitere Schritte an das betroffene Konto.

Eine Lösung ist die Zwei-Faktor-Authentifizierung (2FA). Hier unterscheidet man bei den Schutzmaßnahmen in **Wissen** und **Besitz**. Eine Kombination von Benutzername und Passwort fällt in den Bereich Wissen: Wer sich anmelden will, muss diese wissen. Eine Anmeldung ist von jedem Ort der Welt möglich, unabhängig davon, ob Sie es sind.

So geht's leichter | Passwörter im Griff

Der Zweite Faktor sollte also anders beschaffen sein. Man setzt gerne eine zweite Authentifizierungsschicht ein, die den Besitz von etwas voraussetzt. Beispielsweise die SMS eines Zahlencodes an eine vordefinierte Telefonnummer oder ein so genanntes Token, das eine ständig wechselnde Zahlenkombination anzeigt. Nach der Anmeldung mit Benutzername und Passwort müssen Sie dann noch diesen Zahlencode eingeben.

Für eine erfolgreiche Anmeldung müssen Sie also nicht nur die Zugangsdaten **kennen**, sondern zusätzlich auch noch das Smartphone oder Token **besitzen**, in der Hand haben. Ist das eine kompromittiert, dann hilft das dem Dieb oder Finder nicht. Erst beide Informationen erlauben den Zugriff auf das so geschützte Konto.

2FA bei Facebook

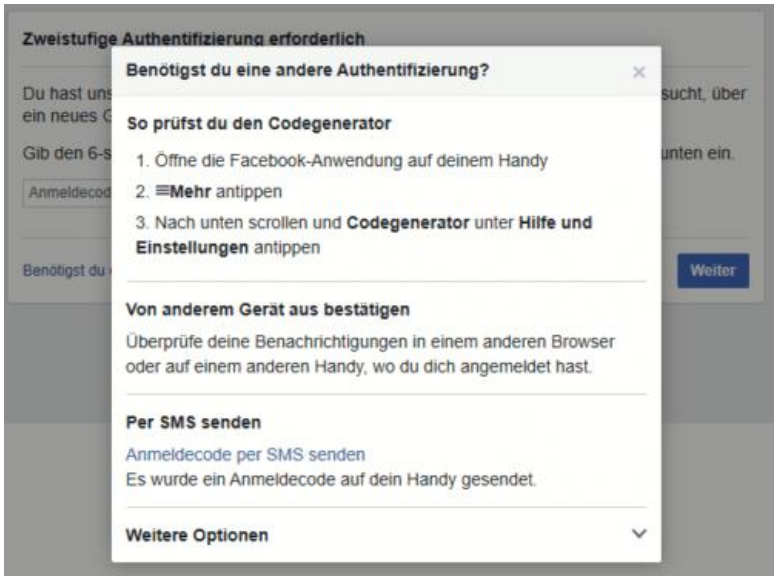
Facebook trifft es immer wieder hart. Oder besser: Die Benutzer trifft es hart. Datenlecks, offen zugängliche Passwörter, Sicherheit ist offensichtlich kein Unternehmensziel. Es macht also Sinn, das selber in die Hand zu nehmen. Facebook bietet die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA).

Kommt ein Unbefugter an das Passwort, dann kann er damit nichts anfangen, denn zur Anmeldung wird dann ein immer wieder wechselnder Code angefordert. Die Einrichtung geht schnell und einfach.

So geht's leichter | Passwörter im Griff

Unter **Einstellungen** > **Sicherheit und Login** können Sie die Zwei-Faktor-Authentifizierung **unter Zweistufige Authentifizierung** einschalten. Im Standard versucht Facebook, Sie von der Verwendung einer Authenticator-App zu überzeugen: Diese kann auf Ihrem Smartphone installiert werden und zeigt Ihnen dann immer den richtigen Code an.

Unabhängiger sind Sie, wenn Sie den Code per SMS schicken lassen. Wenn die Facebook-Anmeldung (auf der Webseite oder der App) den Code abfragt, dann klicken Sie **auf Benötigst Du eine andere Authentifizierung**.



Ein Klick auf **Anmeldeode per SMS** senden löst dann eine SMS mit dem Anmeldecode an die Ihrem Konto hinterlegte Handynummer aus.

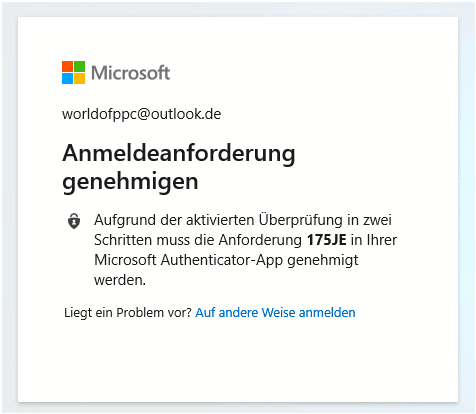
Wollen Sie bei bestimmten Geräten gar keinen Code eingeben, weil Sie sicher sind, dass diese nur in Ihren Händen sind? Dann klicken Sie auf **Autorisierte Logins**, dann sehen Sie die Liste der Geräte, die sich an Ihrem Konto angemeldet haben. Markieren Sie alle Geräte, die keinen Anmeldecode benötigen.

So geht’s leichter | Passwörter im Griff

2FA bei Outlook

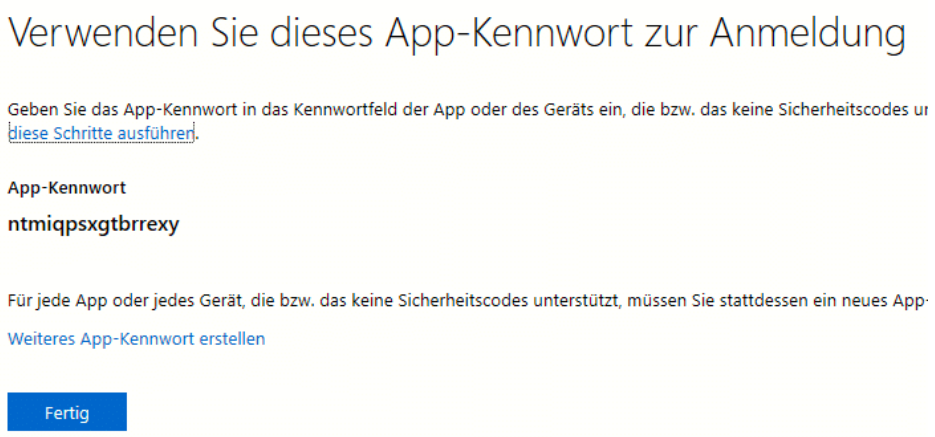
Die Zwei-Faktor-Authentifizierung funktioniert wunderbar, wenn der Zugriff über den Webbrowser stattfindet. Greifen Sie aber mit einem Programm auf das Outlook-Postfach zu, dann kann das Vorgehen von Programm zu Programm abweichen. In der Regel treffen Sie dabei aber nur auf zwei Möglichkeiten. Einmal eingerichtet, ist auch die Mail-Abfrage auf dem PC abgesichert.

Im idealen Fall ist Ihre E-Mail-Software in der Lage, mit der Anforderung eines zweiten Faktors direkt umzugehen und sie zu verarbeiten. Outlook 2016 und 365 wie auch die interne E-Mail-App gehören dazu.



Bei den aktuellen Versionen von Windows wird der Authentifizierungscode der App nur einmalig abgefragt. Direkt danach schaltet sich Windows Hello ein und fordert einmalig die Anmeldung über eine der in Windows hinterlegten Methoden (Wie Fingerabdruck, Gesicht oder Token) an. Wenn Sie die ausgeführt haben, dann wird Windows Hello bei jeder Anmeldung am Postfach als zweiter Faktor verwendet. Deutlich bequemer, als wenn Sie immer Codes eingeben müssen!

So geht’s leichter | Passwörter im Griff



Ältere Versionen von Outlook, Smartphones und andere Programme, die nicht nativ den zweiten Faktor bei der Anmeldung anfordern können, können Sie austricksen. Wechseln Sie wieder in die Sicherheitseinstellungen Ihres Microsoft-Kontos und klicken Sie auf **Zusätzliche Sicherheitsoptionen**.

Unter App-Kennwörter können Sie ein **zufälliges App-Kennwort** erzeugen Das besteht aus einer Kombination aus Ihrem Passwort und einem zufälligen Code. Es ist weder lesbar noch von einem Fremden zu erraten.

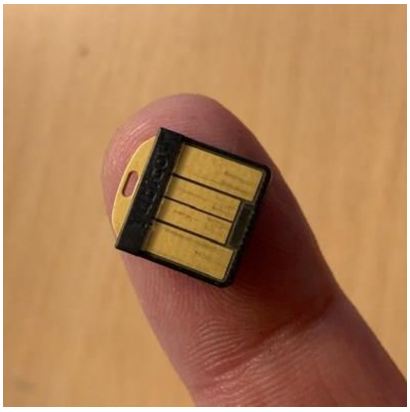
Geben Sie dieses Kennwort statt des Kontokennwortes ein. Das E-Mail-Programm fragt nicht mehr nach dem zweiten Faktor, ein Fremder, der nur Ihr eigentliches Passwort hat, kommt aber nicht an die E-Mails.

2FA und Token für die Anmeldung bei Windows 10

Der einfachste Anmeldeschutz für Windows 10 sind Passwort und PIN. Auch Kamera und Fingerabdruckleser, die in manchen Notebooks und Tablets verbaut sind, erlauben eine sichere und gleichzeitig komfortable Anmeldung am PC. Eher unbekannt, nichts desto trotz aber charmant ist die Verwendung eines Hardware-Tokens. Eine Art Schlüssel, um den

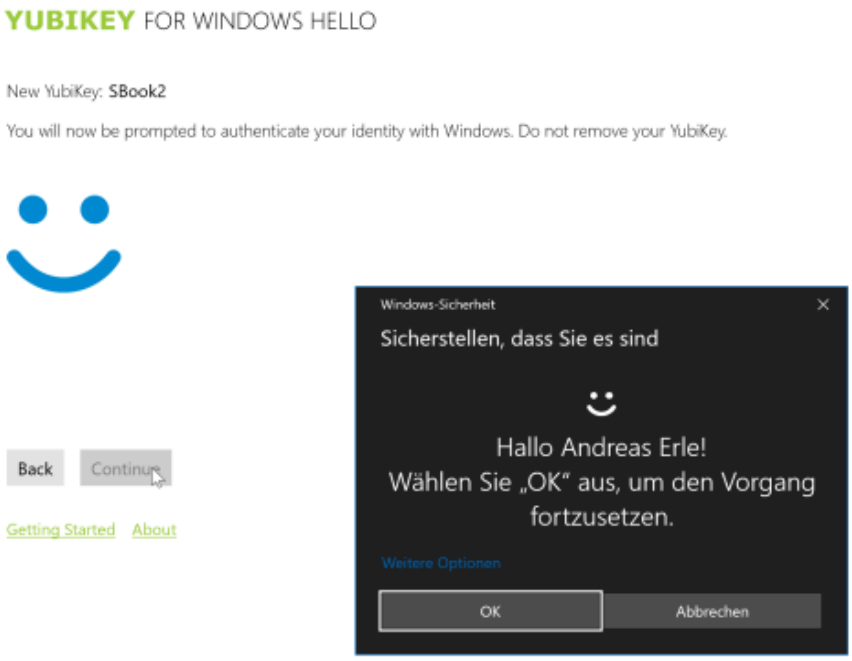
So geht's leichter | Passwörter im Griff

Rechner aufzuschließen. Solche Tokens sind schon für deutlich unter EUR 100,- zu bekommen.



Wo früher noch eine Smartcard oder ein großer USB-Stick nötig waren, hat die Miniaturisierung ebenfalls Einzug gehalten: Security Keys haben heute oft nur die Größe eines Fingernagels und können an einem normalen USB- oder sogar USB-C-Anschluss verwendet werden. Wichtig dabei: Windows 10 muss diese auch unterstützen!

Nicht viele Sicherheit-Tokens unterstützen auch die Anmeldung bei Windows 10 direkt. Yubicos Yubikeys erreichen dies durch eine separate Windows Store-App, die dem Anmeldebildschirm von Windows 10 eine weitere Authentifizierungsmethode hinzufügt.



So geht's leichter | Passwörter im Griff

Einmal konfiguriert wird der Anmeldebildschirm automatisch geschlossen, wenn das Token bei den Anmeldung eingelegt ist. Keine Passworteingabe mehr, denn die Berechtigung für die Anmeldung an Ihren PC ist mit der initialen Einrichtung auf dem Token abgelegt worden.

Noch interessanter ist die Nutzung mit Diensten, die FIDO unterstützen (**F**ast **ID**entity **O**nline). Bei der Registrierung der FIDO-Unterstützung bei einem Dienst wird auf dem Rechner des Benutzers ein Schlüsselpaar generiert. Der öffentliche Schlüssel geht an den Dienst, der private bleibt alleine auf dem Token. Das Token wiederum wird dann noch einmal geschützt, beispielsweise durch einen Fingerabdruck.

Bei der Anmeldung wird dann die Anfrage zur Anmeldung vom Server auf dem PC des Benutzers verschlüsselt und an den Dienst gesendet. Der Dienst kann diese mit dem öffentlichen Schlüssel entschlüsseln und damit die Identität des Anmeldenden bestätigen. Der private Schlüssel bleibt immer beim Benutzer.

Auch diese Anmeldeart wird von Windows 10 direkt unterstützt.

Passwort-Manager

Passwort-Manager sind die Antwort auf Erinnerungslücken. Sie werden im Rahmen der Arbeit am PC und im Internet eine solche Vielzahl von Konten anlegen und benutzen, dass Sie nur zwei Möglichkeiten haben: Entweder sie wählen immer dasselbe, oder Sie schreiben sie auf.

Ersteres ist keine Option, das haben Sie im Rahmen der bisherigen Ausführungen gesehen. Die zweite Variante lässt sich gottseidank auch ohne PostIts realisieren: Es gibt eine Vielzahl von Passwort-Managern, Programmen, die die Passwörter sicher speichern, zwischen Geräten

So geht's leichter | Passwörter im Griff

synchronisieren und Ihnen immer dann zur Verfügung stellen können, wenn Sie sie brauchen.

Vorteile von Passwortmanagern

Was hält Sie davon ab, hinreichend komplexe Passwörter zu verwenden? Ganz weit vorne die Problematik, sich komplexe Zahlen-, Ziffern- und Zeichenfolgen, die sich auch noch unterscheiden sollen, zu merken.

Die analoge Lösung sind tatsächlich die allgegenwärtigen PostIts. Notizzettel, auf denen Sie das Passwort notieren. Diese Rolle können Programme übernehmen, die im Gegensatz zu den Zetteln sicherstellen, dass nur der Berechtigte die Passwörter sehen kann.

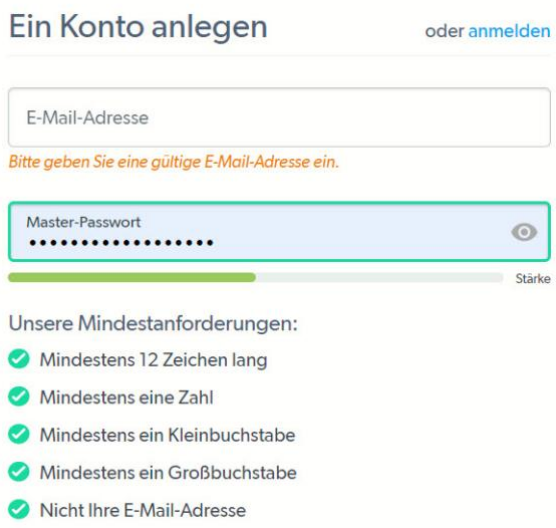
Weiterhin nutzen die Passwort-Manager entweder eigene Speicher oder Standard-Anbieter wie Google oder Dropbox, um die Kennwörter im Rahmen einer Synchronisation auf andere Geräte zu bringen. Was jetzt auf den ersten Blick kritisch erscheint, ist in Wahrheit wohldurchdacht: Die Passwort-Safes, die die Geräte nutzen, werden dabei stark verschlüsselt. Selbst wenn ein Unberechtigter auf diesen Cloudspeicher zugreifen könnte, kann er nicht auf die Daten zugreifen.

Damit löst sich auch das zweite Problem der PostIts: Die Verfügbarkeit, wann immer Sie ein Passwort brauchen. Sei es auf einem anderen PC, dem Tablet oder dem Smartphone. Passwort-Manager synchronisieren beim Start und beim Beenden die aktuellen Passwörter mit dem Cloudspeicher.

So geht's leichter | Passwörter im Griff

Erste Schritte mit einem Password-Manager

Die meisten der Passwort-Manager bieten ein eigenes Konto an, dass dann alle Plattformen (Web, Desktop/Tablet/Notebook, Smartphone) zusammenführt.



Legen Sie dieses auf der Webseite des Herstellers an. Einmalig vergeben Sie dann ein Masterpasswort. Das ist das einzige Passwort, das Sie sich nachher noch merken müssen. Alle anderen landen dann in dem über dieses Masterpasswort verschlüsselten Passwort-Safe.

Wichtig ist hier, dass Sie sich dieses Masterpasswort sicher und nachhaltig merken. Ohne dieses kommen Sie an kein einziges Ihrer Passwörter mehr heran. Eine Möglichkeit kann hier sein, es in einen verschlossenen Briefumschlag in einem physischen Safe, wie die meisten Haushalte ihn mittlerweile haben, abzulegen.

Als nächstes installieren Sie die Passwort-App und/oder die Browsererweiterungen auf jedem der Geräte, auf denen Sie Passwörter verwenden müssen. Viele der Passwort-Manager bieten auch Smartphones-Apps an. Damit haben Sie eine gewisse Unabhängigkeit von einer lokalen Installation. Das Smartphone haben Sie schließlich immer dabei!

Im nächsten Schritt geht es an die Nutzung Ihres neuen Passwort-Managers. Geben Sie Passwörter, die Sie bisher irgendwo anders

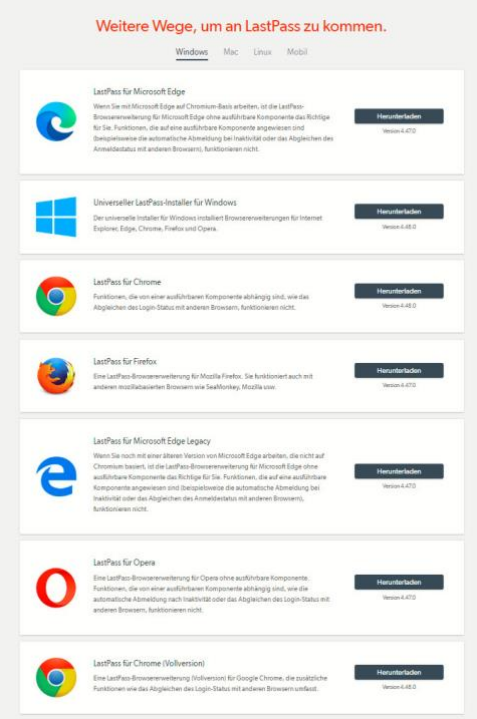
So geht's leichter | Passwörter im Griff

abgelegt haben, ein. Importieren Sie sie aus einem anderen Programm, idealerweise sogar dem Browser.

Manche Passwort-Manager überprüfen Ihnen dann die Passwörter auf ihr Qualität und gegebenenfalls sogar darauf, ob sie bereits einem Hack zum Opfergefallen sind und warnen Sie davor.

Diese Sonderfunktionen variieren von Programm zu Programm. Es kann durchaus Sinn machen, vor der endgültigen Auswahl einmal verschiedene Passwort-Manager zu vergleichen, bevor Sie viel Arbeit in die Pflege Ihrer Passwort-Datenbank investieren. Wir stellen Ihnen die fünf besten Passwort-Manager vor:

LastPass



LastPass (https://lastpass.com/de) ist mit einer der beliebtesten Passwort-Manager. Unter anderem deshalb, weil er in der kostenlosen Variante schon eine Menge Funktionen mitbringt.

Die kostenpflichtige Version bietet dann für ab USD 3,- im Monat das Teilen von Passwörtern mit anderen Benutzern an, einen 1GB großen, verschlüsselten Seitenspeicher und die Möglichkeit, ein Hardwaretoken als Schutz des Passwort-Tresors zu verwenden.

Unter https://lastpass.com/download finden Sie die verschiedenen Versionen für alle Desktop-Betriebssysteme und die Plugins für die gängigen Webbrowser. Ganz rechts in der Menüleiste über den Links können Sie

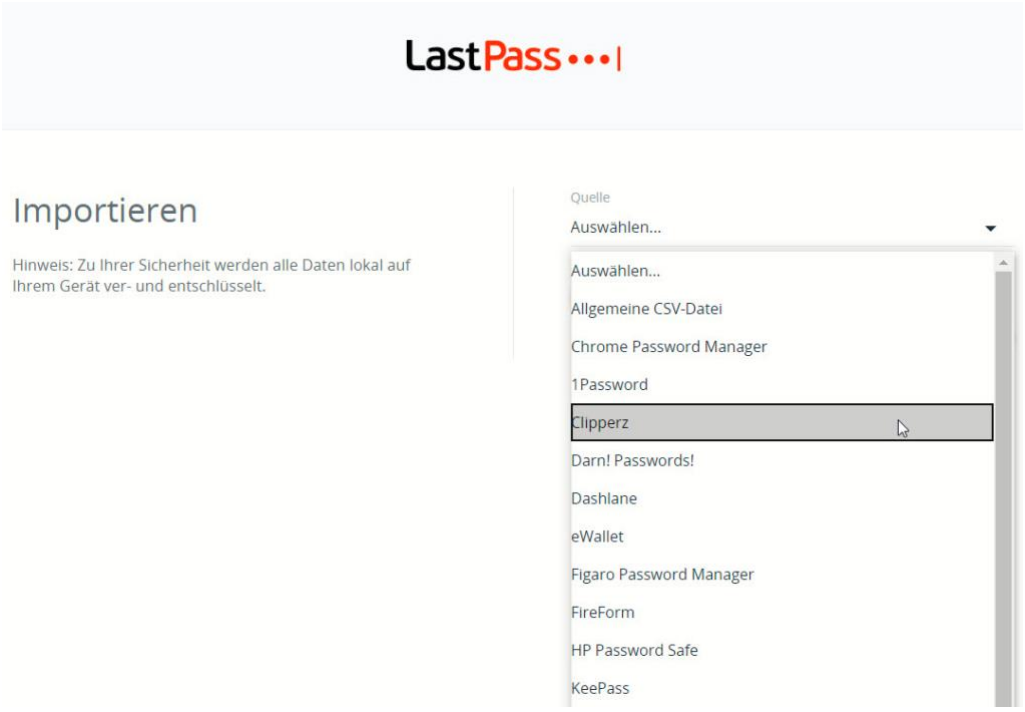
So geht's leichter | Passwörter im Griff

auf **mobil** klicken und von dort aus direkt in den App Store Ihres Smartphones gelangen.

Beim ersten Start der LastPass Desktop-App zeigt Ihnen diese alle unsicher gespeicherten Passwörter an, die auf Ihrem Rechner gefunden wurden und bietet deren Import in LastPass an. Das sind meist Passwörter aus dem alten Internet Explorer und WLAN-Zugänge.

Import der Passwörter aus einer Datei

LastPass bietet die direkte Möglichkeit, über die Browser-Erweiterung gespeicherte Passwörter zu importieren, die sie in einer Datei vorliegen haben. Das kann eine Excel-Tabelle sein, ein Export aus einem anderen Passwort-Manager oder anderen Programm.



.

So geht's leichter | Passwörter im Griff

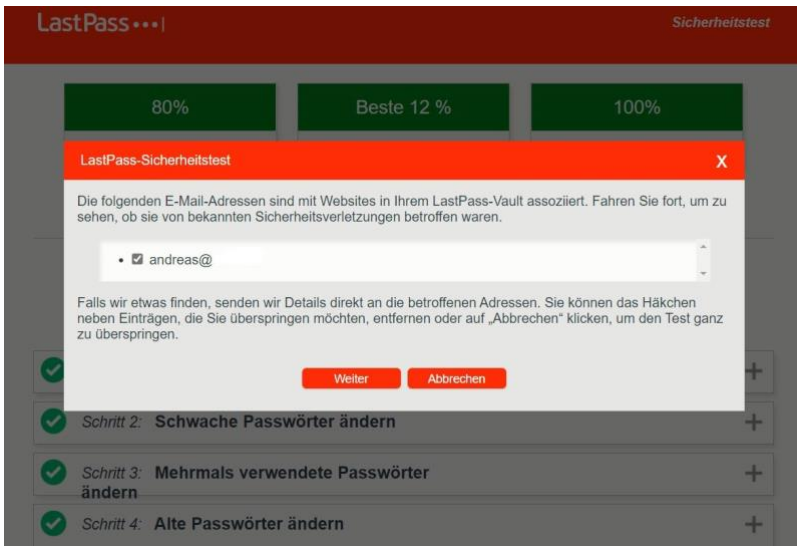
Dazu gehören die meisten anderen Passwort-Manager, ein Umstieg von einem anderen Produkt auf LastPass ist also relativ einfach zu bewerkstelligen.

In der Browser-Erweiterung klicken Sie dazu auf **Kontooptionen** > **Erweitert** > **Importieren** und wählen Sie die Quelldatei aus. Nach dem Import können Sie die Passwörter dann in LastPass auf allen Geräten verwenden.

Auf dem selben Weg können Sie übrigens Ihre LastPass-Datenbank auch exportieren. Sie sollten aber mit einer solchen Export-Datei extrem vorsichtig umgehen: Wer diese in die Finger bekommt, der hat Ihre Passwörter zur Verfügung. Sie sollten Sie also erstellen, direkt verwenden und dann direkt wieder endgültig löschen.

Sicherheitstest Ihrer aktuellen Zugangsdaten

Eine tolle Funktion von LastPass ist der Sicherheitscheck: Der Untersucht Ihr Zugangsdaten auf verschiedene Schwächen.



So geht's leichter | Passwörter im Griff

Dazu gehört die Prüfung, ob diese in einem Hack verwendet wurden. Doppelte und schwache Passwörter werden ebenfalls identifiziert und können dann direkt geändert werden.

Automatisches Ausfüllen von Passwörtern

Das Automatische Ausfüllen von Webformularen und Anmelde-Bildschirmen ist recht einfach. Mit der Browsererweiterung von LastPass fügt der Browser eines Desktop-Gerätes diese auf bekannten Seiten automatisch ein.

Damit das auch bei Smartphones funktioniert, müssen Sie die so genannten AutoFill-Optionen aktivieren. Die finden Sie in den Eingabeeinstellungen (Sprache und Tastatur) bei Android, unter iOS bei **Passwörter & Accounts** > **Automatisch ausfüllen**. Hier muss LastPass aktiviert werden, damit die Benutzerdaten dann im mobilen Browser eingetragen werden können.

1Password

1Password (https://1password.com/) bietet im Gegensatz zu LastPass die Möglichkeit, Ihre Passwort-Datei nicht nur in der Cloud, sondern auch lokal zu speichern. Wenn Sie also nicht das nötige Vertrauen zu den Clouddiensten haben, dann können Sie darauf verzichten. Das allerdings bedeutet dann manuellen Aufwand, wenn Sie die Passwörter auf verschiedenen Geräten zur Verfügung haben wollen.

1Password bietet eine kostenlose Testversion, die Sie 30 Tage lang nutzen können. Danach müssen Sie sich für eines der Bezahlmodelle entscheiden oder die Nutzung einstellen. Wichtig bei der Anmeldung: Wählen Sie **Persönlich & Familie** aus, Teams & Business

So geht's leichter | Passwörter im Griff

Als erstes legen Sie ein Konto bei 1Password an. Nach Abschluss dieses Prozesses bekommen Sie einen Barcode angezeigt, der extrem wichtig ist: Er dient der Anbindung von Anwendungen und Apps an Ihr Konto. Ohne diesen Code sind sie verloren, heben Sie ihn also gut auf!

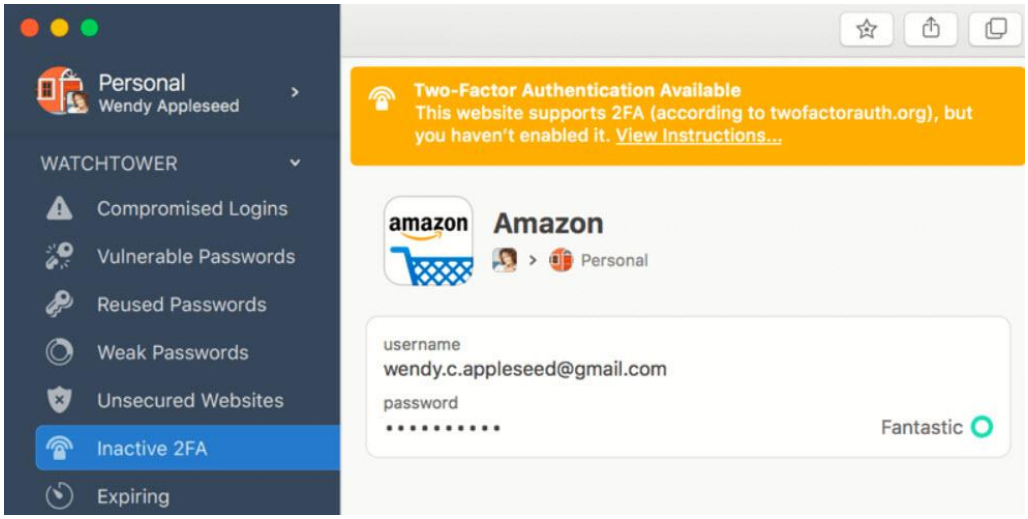
Jedes Gerät, mit dem Sie auf 1Password zugreifen, wird dann mittels des Setup-Codes eingerichtet. Damit haben Sie – wenn Sie sich nicht für eine lokale Speicherung der Passwörter entschieden haben – auch die Synchronisation zwischen Geräten eingerichtet. Ob Browser-Erweiterung, Desktop-Software oder Android- und iOS-App: Die Passwörter sind dann umgehend auf allen Geräten verfügbar.

Watchtower: Der Sicherheitscheck

Ihr Passwörter sind im Laufe von vielen Jahren gewachsen. Bei manchen Diensten haben Sie sich schon lange Zeit nicht angemeldet, ja vielleicht sogar vergessen, dass Sie dort ein Konto haben. Die Watchtower-(Wachturm) Funktion von 1Password erlaubt die Überprüfung Ihrer gespeicherten Passwörter.

Neben der Kontrolle auf bereits durch einen Hack kompromittierte und schwache Passwörter bekommen Sie in der Auswertung auch einen Hinweis darauf, welcher von Ihnen benutzte Dienst die Zwei-Faktor-Authentifizierung (2FA) anbietet. Immer mehr Dienste bieten diese zusätzliche Sicherheitsstufe nach und nach an. Die Funktion spart Ihnen also das manuelle Nachhalten der Enzwicklung.

So geht’s leichter | Passwörter im Griff



Eingeben und Verwenden von Passwörtern

In den meisten Fällen werden Sie mit einer der Browser-Erweiterungen von 1Password arbeiten. Diese erkennt ein Passwortfeld und fragt direkt ab, ob Sie das eingegebene Passwort in 1Passwort speichern wollen. So, wie die Standard-Browser es bei der Speicherung in ihren eigenen Datenbanken auch machen.

Wechseln Sie auf eine Seite, die 1Passwort schon kennt, dann werden Benutzername und Kennwort schon voreingetragen und sie müssen nur noch die Eingabe bestätigen.

Damit das auch bei Smartphones funktioniert, müssen Sie die so genannten AutoFill-Optionen aktivieren. Die finden Sie in den Eingabeeinstellungen (Sprache und Tastatur) bei Android, unter iOS bei **Passwörter & Accounts** > **Automatisch ausfüllen**. Hier muss LastPass aktiviert werden, damit die Benutzerdaten dann im mobilen Browser eingetragen werden können.

So geht's leichter | Passwörter im Griff

Integrierter Passwort-Generator

Bei dem Anlegen von neuen Konten kann 1Passwort eine Hilfe bei der Auswahl des Passwortes sein: Der integrierte Passwort-Generator schlägt Ihnen ein sicheres Passwort vor, dass Sie auf Wunsch direkt übernehmen können.

Das macht Sinn, wenn Sie tatsächlich einzig und allein auf Geräten arbeiten können, die 1Password installiert haben. Dort füllt das Programm ja das meist aus wilden Buchstaben-, Zahlen und Ziffernkombinationen bestehende Passwort automatisch ein. Wenn Sie auf das manuell abtippen müssten, wäre das arg aufwändig.

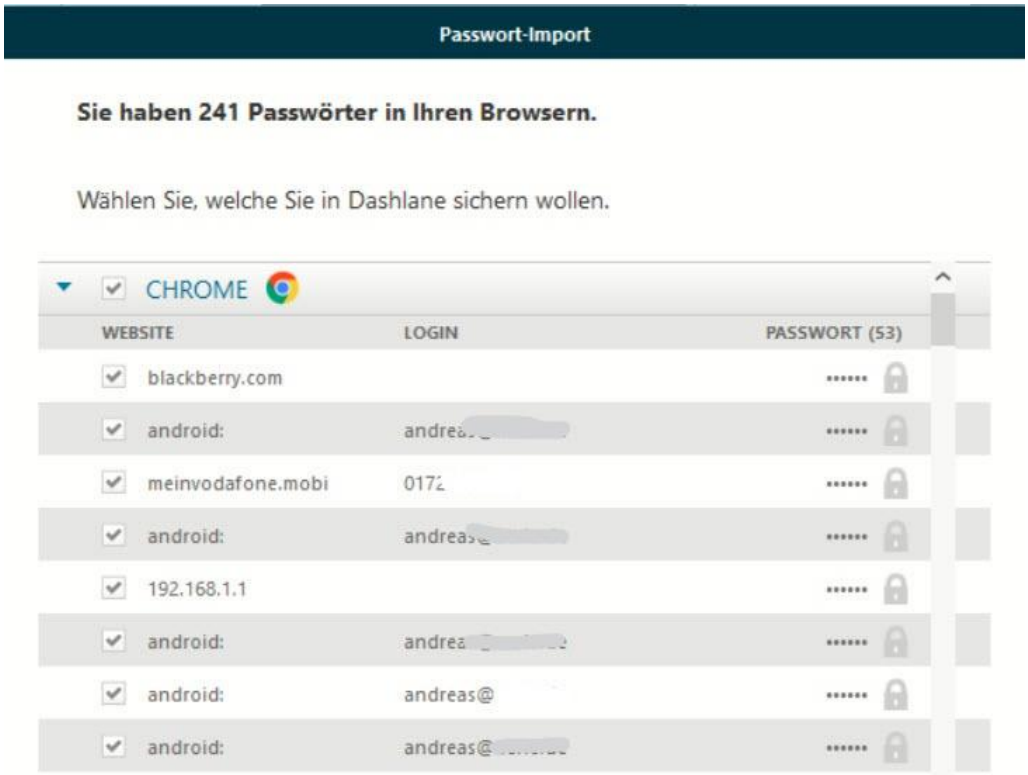
Dashlane

Für viele Anwender ist der kostenlose Passwort-Manager Dashlane (https://www.dashlane.com/de) der vor allem durch seine Funktionsvielfalt auffällt. Diese lässt sich allerdings nach den ersten kostenlosen 30 Tagen durch ein Abo (ab EUR 3,33/Monat) erweitern, wenn Sie mehr als 50 Passwörter oder mehr als ein Gerät verwenden wollen. Laden Sie die Desktop-App herunter, installieren und starten Sie sie.

Als erstes müssen Sie nun ein kostenloses Konto anlegen. Das dort vergebene Passwort dient als Masterpasswort, das die gespeicherten Passwörter verschlüsselt und damit sichert. Das dürfen Sie nicht verlieren oder vergessen! Eine Besonderheit bietet Dashlane bei der Einbindung in Windows 10: Statt des Masterpasswortes können Sie in den Einstellungen festlegen, dass stattdessen Windows Hello, die biometrische Anmeldemethode genutzt werden kann.

So geht's leichter | Passwörter im Griff

Dashlane erkennt automatisch die in den Browsern gespeicherten Kennwörter und bietet Ihnen an, diese zu importieren. Das bringt vor allem den Vorteil, dass Sie auch vergessen geglaubte Zugänge wieder einsehen können und die Passwörter sehen können. Nicht jeder Browser unterstützt das.



Dashlane bietet beim ersten Start schon die Möglichkeit, alle unterstützten Browser-Erweiterungen zu installieren. Diese werden automatisch heruntergeladen, natürlich können Sie dies aber später auch noch nachholen, indem Sie diese unter **Erweiterungen** auswählen.

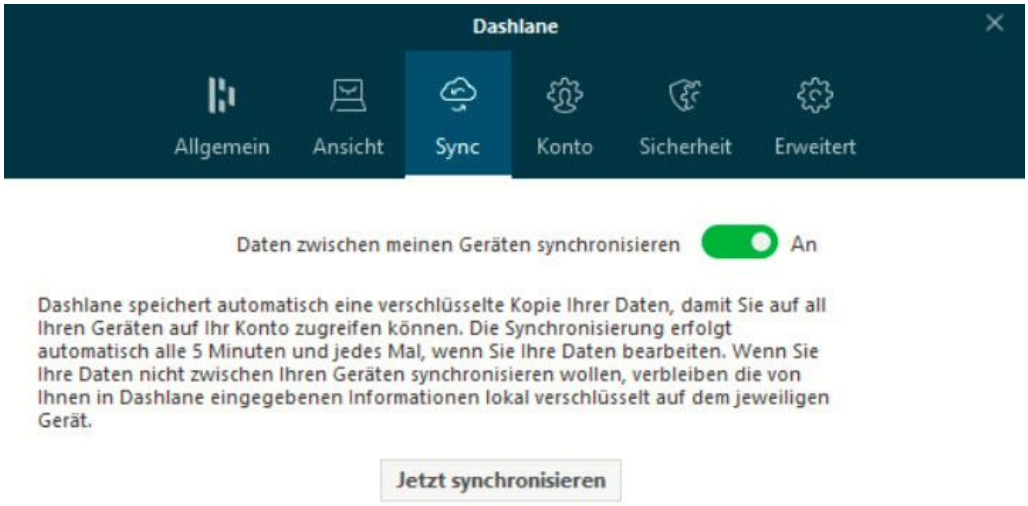
Import und Synchronisation

Dashlane bietet den Import von Passwörtern aus bestehenden Quellen an. Dazu gehören die Browser, aber eben auch verschiedene Dateiformate von anderen Passwortmanagern und Textdateien. Genauso

So geht's leichter | Passwörter im Griff

können Sie Ihren Datenbestand aus Dashlane exportieren und dann in anderen Programmen weiterverwenden. Die Lösung ist also sehr offen.

Dashlane bietet einen eigenen Synchronisationsservice an, der die Passwortdateien auf allen Geräten synchron hält. Wichtig dabei zu wissen: Im Gegensatz zu manch anderem Programm erfolgt die Synchronisation nicht bei jeder Änderung, sondern in einem festen Rhythmus von 5 Minuten. Im Extremfall kann es also bis zu 10 Minuten dauern, bis eine Änderung auf dem Desktop auch auf dem Smartphone sichtbar ist.



Umfangreiche Sicherheitsfunktionen

Analysiert auf Wunsch Ihre komplette Passwort-Datenbank nach der Sicherheit und Angreifbarkeit der Einträge. Im integrierten Identitäts-Dashboard können Sie sich sortiert nach dem Sicherheitsmangel angesehen, welches Konto welchen Mangel hat.

So geht's leichter | Passwörter im Griff

Noch mehr; Auf Wunsch können Sie bis zu fünf-Adresse eingeben, die von Dashlane im Darknet überwacht werden. Sobald diese Adressen in einem neuen Hack oder bei einer anderen verdächtigen Aktion verwendet werden, bekommen Sie eine E-Mail und können schnell reagieren. Ein regelmäßiger Blick in die Auswertungen erhöht die Sicherheit Ihrer Online-Konten beträchtlich, und da die Apps Sie immer wieder darauf hinweist, fällt das leicht.

Viele Zusatzfunktionen

Neben der reinen Passwortverwaltung kann Dashlane im Passworttresor noch eine Vielzahl weiterer Elemente ablegen: Neben Passwörter können Sie die persönlichen Daten für Webformulare, Notizen, Ihre Kreditkarten und EC-Karten, Ausweise und Belege sicher und vor fremdem Zugriff geschützt ablegen. Eine All-in-One-Lösung quasi.

Avira Password Manager

Ein weiterer verbreiteter Password-Manager kommt von den Machern der Antivirenlösung Avira (https://passwords.avira.com/). Der in der Basisversion kostenlose Avira Password Manager wird vor allem als Browserversion vermarktet, die über die Erweiterung der gebräuchlichen

So geht's leichter | Passwörter im Griff

Browser fungiert. Für Android und iOS gibt es dann die entsprechenden Apps. Auch wenn die Funktionalität eher einfach ist, eine Besonderheit bringt der Dienst mit: Sie müssen nicht zwangsläufig ein neues Konto anlegen, sondern können beispielsweise auch Ihr Facebook-Konto als Identifikation verwenden.

Die Sicherung des Passworttresors wird aber trotzdem durch ein separat zu vergebendes Masterpasswort erreicht. Sie müssen also keine Sorge haben, dass Facebook an Ihre Passwörter kommen kann.

Neben den üblichen Funktionalitäten für die Passwortverwaltung können Sie eine Sicherheitsanalyse über alle gespeicherten Passwörter laufen lassen und Zahlungsdaten in einem separaten Bereich, dem Wallet, speichern.

Sticky Password

Eine nette Alternative zu Synchronisation der Passwortdatei über die Cloud bietet der kostenlose Passwort-Manager Sticky Password (https://www.stickypassword.com/de/). Der bietet neben der Synchronisation über die eigenen Cloud-Server auch dir Möglichkeit, lokal übe WLAN mit anderen Geräten zu synchronisieren.

Damit können alle Geräte, die sich in Ihrem Netzwerk aufhalten, aktuell gehalten werden. Und das ohne, dass die Passwort-Datei Ihr Netzwerk verlässt. Diese Funktion steht allerdings nur in der kostenpflichtigen Version zu Verfügung. Die kostet EUR 36,95 im Jahr.

So geht’s leichter | Passwörter im Griff

Neben den Webkonten können Sie in Sticky Password auch Programmkonten verwalten. Wenn Sie sich bei einem Programm auf Ihrem PC mit Zugangsdaten anmelden müssen, dann können Sie auch diese speichern und automatisch vorausfüllen lassen.

Eine weitere Besonderheit ist die Funktion zum Teilen von Inhalten mit anderen Sticky Password-Benutzern. Damit können Sie Passwörter teilen, ohne die Sicherheit zu verringern und über E-Mail oder Messenger-Dienste ein Risiko einzugehen.