AUSGABE 26
Juli 2022

SICHERE PASSWÖRTER

Bildquelle: Vitalii Vodolazskyi / Shutterstock.com

Einzigartig und komplex

biallo.de
Ihr Geld verdient mehr.

Sichere Passwörter

Einzigartig und komplex

von Annette Jäger

Bildquelle: akimov.de

Mal ehrlich, wie viel Mühe geben Sie sich bei der Vergabe eines Passworts, wenn Sie im Internet einkaufen? Verwenden Sie überall dasselbe Passwort, das Sie schon auswendig können? Oder setzen Sie auf eine leicht zu merkende Zahlenreihe? Wenn ja, dann sollten Sie diesen Text lesen. Denn Ihre Methode der Passwortvergabe erfüllt eher nicht die Sicherheitsstandards und Cyber-Kriminelle haben so leichtes Spiel, an Ihre persönlichen Daten zu gelangen

Wer viel im Internet unterwegs ist, dabei Online-Banking nutzt, Einkäufe tätigt, auf Social Media-Plattformen aktiv ist, vergibt ständig Passwörter für neue Accounts. Haben Sie mal alle zusammengezählt? Da kommen leicht über 100 zusammen. Ein sicheres Passwort ist dabei das A&O, denn Kriminelle können leicht ein unsicheres Passwort knacken, persönliche Daten abgreifen und Sie schädigen. Verbraucher unterschätzen diese Gefahr häufig, dabei ist sie immanent. Professor Christoph Meinel, Direktor des Hasso-Plattner-Instituts in Potsdam und Leiter des Fachgebiets Internet-Technologien und Systeme, vergleicht ein unsicheres Passwort mit dem Steckenlassen eines Schlüssels in der Haustür – es ist eine Einladung zum Identitätsdiebstahl.

Lesen Sie auf den folgenden Seiten, wie Passwörter geknackt werden können, wie Sie ein sicheres Passwort vergeben, was Passwortmanager leisten und wie Sie im Schadensfall vorgehen.

Wie sicher ist mein Passwort?

Es gibt tatsächlich so etwas wie die Top-Ten der beliebtesten deutschen Passwörter. Schon allein die Tatsache, dass sich so eine Liste erstellen lässt, zeigt, dass sehr viele Deutsche dieselben Passwörter nutzen, was ja den Sinn eines Passworts, das individuell und einzigartig sein soll, ad absurdum führt.

Bildquelle: geen graphy / Shutterstock.com


Bildquelle: Pixels Hunter / Shutterstock.com

Überprüfen Sie selbst, ob Ihres dazugehört:

Top Ten deutscher Passwörter 2021:

1. 123456
2. passwort
3. 12345
4. hallo
5. 123456789
6. qwertz
7. schatz
8. basteln
9. berlin
10. 12345678

(Quelle: Hasso-Plattner-Institut: https://hpi.de/pressemitteilungen/2021/die-beliebtesten-deutschen-passwoerter-2021.html)

Mit einem solchen Passwort machen Sie es Kriminellen natürlich einfach, dieses zu knacken und so Zugang zu Ihren persönlichen Daten zu erhalten. Neben der Einfachheit eines Passworts ist die zweite Gefahr die Häufigkeit der Vergabe: Wenn Sie ein und dasselbe Passwort für verschiedene Konten vergeben, dann sind Sie gleich mehrfach geschädigt, wenn Ihr Passwort geknackt wird.

Passwörter hacken – so groß ist die Gefahr

Viele unterschätzen die Gefahr, die von einem unsicheren Passwort ausgeht. Das Bundeskriminalamt erhebt jedes Jahr das sogenannte Bundeslagebild zur Cyberkriminalität. Hier ein paar Fakten aus dem Bericht 2021, die zeigen wie immanent die Gefahr ist, selbst zum Opfer zu werden:

- Die Anzahl erfasster Cyberstraftaten steigt weiter an – im Jahr 2021 um über zwölf Prozent.
- Die Aufklärungsquote liegt knapp unter 30 Prozent.
- Die Underground Economy* boomt. Umfang und Qualität der angebotenen inkriminierten Waren und Dienstleistungen nehmen weiterhin zu. Gleichzeitig sinken täterseitige Eintrittsbarrieren
- Cybercrime verursacht Schäden in Milliardenhöhe – Tendenz weiter steigend

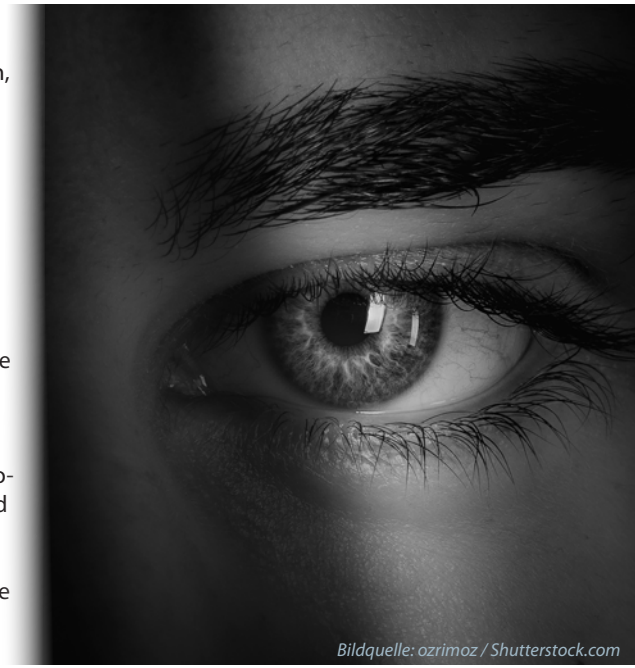
Das Fazit für das Jahr 2021: Die Zahl der Cybercrime-Vorfälle ist gestiegen, die Täter bedienen sich vielfältiger Tatgelegenheiten, die ihnen die Underground Economy bietet. Die Corona-Pandemie hat mit ihrem Schub an Digitalisierung wie ein „Beschleuniger" für Cybercrime gewirkt.

(Quelle: Cybercrime. Bundeslagebild 2021. Bundeskriminalamt.)

*Underground Economy: „Die Underground Economy (UE) bezeichnet die Gesamtheit der Plattformen und Services, welche von (Cyber-) Kriminellen genutzt wird, um Daten, Tools, Jobs und relevantes Täter-Know-How anzubieten oder in Anspruch zu nehmen. Dieses Angebot bildet die Grundlage vieler Straftaten im Cyber-Bereich." Quelle: Cybercrime. Bundeslagebild 2021. Bundeskriminalamt.

So gehen Täter vor

Man mag sich als Internetnutzer fragen, welches Interesse Cyberkriminelle haben könnten, einen ganz persönlich auszuspähen und Daten zu klauen. Schließlich hat man doch finanziell nicht viel zu bieten und schätzt sich selbst als eher unbedeutend ein, in der großen weiten Welt des Internets. Doch diese Denkweise trifft nicht das Vorgehen von Tätern. Denn tatsächlich wird kaum ein Betrüger ganz gezielt die Daten einer einzelnen Person knacken. Das geschieht vielmehr im großen Stil und voll automatisiert. Passwörter hacken oder knacken ist das Geschäftsmodell von Kriminellen, und entsprechend organisiert und professionell läuft das ab. Und je „schwacher" ein Passwort ist – also zum Beispiel eine chronologische Zahlenfolge – desto leichter wird es erbeutet.



Bildquelle: ozrimoz / Shutterstock.com

Bildquelle: Imilian / Shutterstock.com

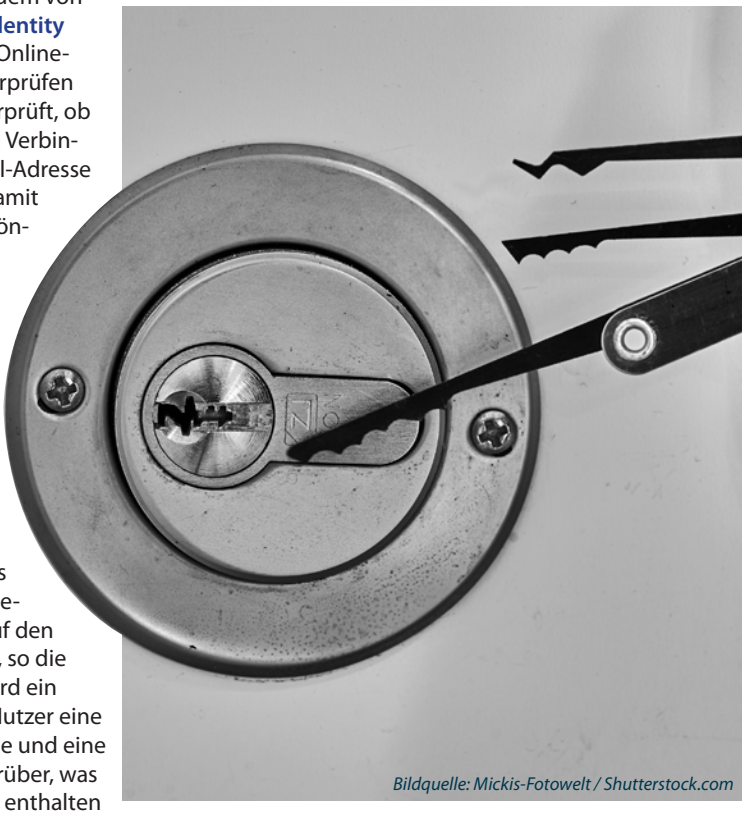
Persönliche Daten gelangen häufig über Datenlecks ins Internet und sind dort in entsprechenden Foren frei verfügbar (siehe Underground Economy). Solche Datenlecks können zum Beispiel durch Sicherheitslücken in Unternehmen entstehen, wenn Daten unachtsam auf Servern abgelegt werden und dann gezielt von Hackern gestohlen und verkauft werden. Oft werden sie aber auch zum freien Missbrauch ins Internet in Foren gestellt, wo Kriminelle sie abgreifen können. Die Täter arbeiten oft mit spezieller Software. So sind Roboter gefüttert mit ganzen Wörterbüchern und können über „Ausprobierattacken" ganze Foren auf Wort- und Zahlenkombinationen in Sekundenschnelle absurfen, ob es an einer Stelle Übereinstimmung mit einer Passwortkombination gibt. Somit haben sie in Sekundenschnelle Zugang zu persönlichen Daten.

Passwort geknackt? Der Identity Leak Checker verschafft Klarheit

Das Hasso Plattner-Institut (HPI) der Universität Potsdam erfasst Millionen von Datenlecks und geht davon aus, dass täglich persönliche Daten im Internet geklaut werden. Ob man selbst Opfer eines Datendiebstahls geworden ist, lässt sich mit dem von dem Institut entwickelten **Identity Leak Checker (ILC)**[1], einem Online-Sicherheitscheck, leicht überprüfen – kostenlos. Dabei wird überprüft, ob bereits persönliche Daten in Verbindung mit der eigenen E-Mail-Adresse im Internet kursieren und damit auch missbraucht werden können. Die Sicherheitsforscher ermöglichen den Abgleich mit mittlerweile mehr als 12,7 Milliarden gestohlener Identitätsdaten, die im Internet verfügbar sind. Dabei liegt der Fokus auf Leaks, bei denen deutsche Nutzer betroffen sind. „Die E-Mail-Adresse ist perfekt zum Abgleich geeignet, da sie der Quasi-Standard ist als Nutzername bei der Registrierung digitaler Identitäten auf den verschiedenen Plattformen", so die Erläuterung des Instituts. Wird ein Treffer gefunden, erhalten Nutzer eine Antwortmail auf Ihre Anfrage und eine genaue Aufschlüsselung darüber, was alles in dem jeweiligen Leak enthalten war und wie Betroffene nun vorgehen sollten. Die Änderung des Passworts ist dabei zentraler Bestandteil.

Tipp:

Nutzen Sie den Dienst in regelmäßigen Abständen, denn es gibt ständig neue Leaks von Identitätsdaten.



Bildquelle: Mickis-Fotowelt / Shutterstock.com

Fazit:
Wer ein schwaches Passwort nutzt – eine einfache Zahlenreihe oder Tastenkombinationen – geht ein erhebliches Risiko ein, dass das Passwort gehackt wird. Denn Täter probieren natürlich erst die einfachen Schlüssel aus, um eine digitale Identität zu erbeuten.

So erstellen Sie ein sicheres Passwort

Ungeeignete Passwörter

Einzigartig und komplex – das sind die Maßgaben für ein sicheres Passwort. Damit scheiden alle Passwörter aus, die zum Beispiel

- **Namen** von Familienmitgliedern, Freunden, des Haustieres, des Lieblingssängers oder ähnliches enthalten
- persönliche **Geburtsdaten** enthalten
- eine persönliche Verbindung zu Ihnen haben
- **Wörter** sind, die in einem Wörterbuch vorkommen
- reine **Zahlenreihen** sind wie 123456
- reine **Buchstabenreihen** sind wie vcxy, die nebeneinander auf einer Tastatur liegen
- eine Kombination sind aus aufeinanderfolgenden und offensichtlichen Buchstaben- und Zahlenreihen wie 12345 vcxy

Tipp:

Ebenfalls sollten Sie niemals dasselbe Passwort für verschiedene Accounts verwenden, sondern vielmehr für jedes Nutzerkonto ein eigenes Passwort erstellen.

Bildquelle: akimov.de

Geeignete Passwörter

Es gibt klare Kriterien, was ein sicheres Passwort ist. Der aktuellste Rat von Experten lautet: Die Länge macht`s. Wenn ein Passwort 20 Zeichen enthält, ist das viel zu mühevoll, es zu knacken.

Bildquelle: bcoelho / Shutterstock.com

Ein sicheres Passwort…

- ist mindestens 15 und besser 20 Zeichen lang
- enthält Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Beispiel: 3ej4yykOiwbi&XrgI§Zo

Anstatt ein völlig willkürliches Passwort zu nutzen, könnten Sie sich auch Eselsbrücken bauen. Setzen Sie zum Beispiel die jeweils ersten Buchstaben in einem Satz aneinander und ersetzen dann manche Buchstaben mit Zahlen und Sonderzeichen. Allerdings sollte der Satz ein selbst ausgedachter sein und keine Liedzeile, ein bekanntes Zitat oder ähnliches.

Beispiel: „Ich nutze die Plattform biallo.de, weil ich dort wertvolle Informationen rund um meine privaten Finanzen erhalte." Die ersten Buchstaben der Worte reihen sich wie folgt aneinander: IndPbwidwIrumpFe. Nun könnten Sie die beiden „I" durch eine 1 ersetzen, weil sie ähnlich aussehen. Oder das „w" durch die Zahl 23, weil es an dieser Stelle im Alphabet steht. Und aus dem „d" wird ein „&"-Zeichen.
Dann lautet das neue Passwort so: 1ndPb23i&w1rumpFe – komplex und einzigartig.

Es gibt natürlich nie die 100-prozentige Sicherheit, dass nicht auch ein vermeintlich sicheres Passwort zu knacken ist und Sie dadurch Schaden erleiden. Aber ein sicheres Passwort erhöht das Sicherheitsniveau bedeutend.

Tipp:

Speichern Sie niemals auf Ihrem Computer oder auf Ihrem Smartphone Passwörter in ungeschützten Dateien. Verschicken Sie Passwörter nicht per E-Mail, SMS oder auf einem ähnlichen Weg.

Oftmals dient ein Fingerabdruck als Passwort. Das ist eine andere sichere Variante eines Passworts, die häufig bei Apps auf Smartphones Verwendung findet.

Sicheres Passwort:
Kein Schutz vor Phishing

Auch wenn Sie noch so sichere Passwörter benutzen – sie stellen leider keinen Schutz vor Phishing dar. Mit dem Begriff wird das Ausspähen und Klauen von Passwörtern bezeichnet. Das geschieht oft über gefälschte E-Mails. Sie sehen den echten Mails, die man von Banken, Bezahlsystemen im Internet oder ähnlichem bekommt, zum Verwechseln ähnlich. Meist wird man im Betreff verunsichert, weil dort steht, dass entweder eine Rechnung offen ist oder ein Konto gesperrt wird. In der Mail wird man dann aufgefordert, auf einen Link zu klicken, einen Anhang zu öffnen oder seine Zugangsdaten einzugeben. Und schon haben die Kriminellen Zugriff auf die persönlichen Daten – und auf ein vielleicht hochkomplexes Passwort. Deshalb gilt: öffnen Sie nie unbekannte Anhänge!

Bildquelle: SoftLight / Shutterstock.com

Passwörter verwalten – so funktionieren Passwortmanager

Sichere Passwörter, die komplex sind und keinem Muster folgen, kann man sich natürlich nicht in großer Menge merken. Deshalb empfehlen Experten, unbedingt mit einem Passwortmanager zu arbeiten. Das ist eine Software, die man sich herunterladen kann und die sich dafür eignet, die eigenen Passwörter sicher zu verwalten, aber auch, um sichere Passwörter zu generieren. Es gibt kostenlose Varianten und solche, die zwischen zehn und 40 Euro im Jahr im Abonnement kosten und dann einige Funktionen mehr aufweisen. Die Sicherheitsstandards dieser Programme sind sehr hoch. Dennoch gibt es Experten, die davon abraten, sehr sensible Passwörter, etwa zum Online-Banking hier zu hinterlegen.

Die Handhabung der Programme ist einfach. Man kann beispielsweise in dem vom Bundesamt für Sicherheit und Informationstechnik (BSI) empfohlenen Programm Keepass Ordner anlegen für verschiedene Themen, zum Beispiel Einkaufen, Social Media, Reise, E-Mail und unter dem Ordner die jeweiligen, bereits existierenden Passwörter für die einzelnen Nutzerkonten speichern. Beim Anlegen eines neuen Passworts schlägt das Programm ein sicheres, starkes Passwort vor, das man einfach über die Funktion Copy&Paste übernehmen und im jeweiligen neu eröffneten Nutzerkonto einfügen kann. Dem neu generierten Passwort im Passwortmanager ordnet man einen eigenen Namen zu, zum Beispiel den der genutzten Shopping Plattform, und kann es so bei Bedarf jederzeit wieder abrufen.

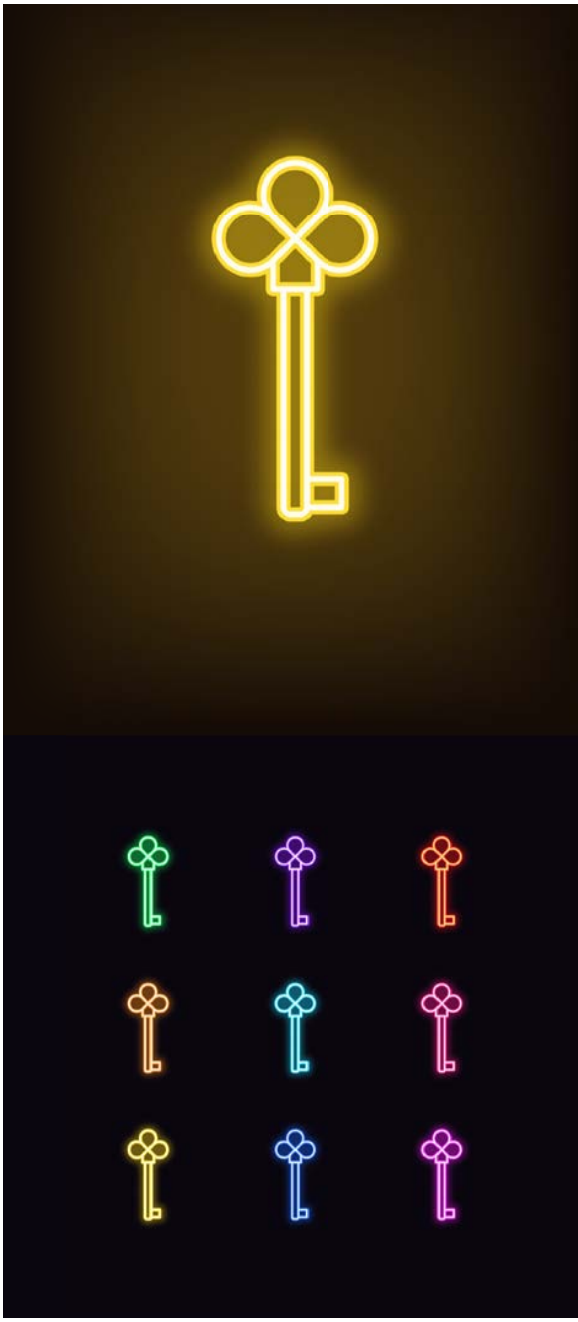
Bildquelle: Elena Abrazhevich / Shutterstock.com

Das gute an den Passwortmanagern ist, dass Sie sich das Programm auf das Smartphone, den PC, das Tablet laden können und sich das Ganze auch noch synchronisieren lässt, so dass Sie auf allen Geräten Zugriff auf Ihre Passwörter haben. Eines müssen Sie sich allerdings merken: Das Masterpasswort, mit dem Sie sich beim Passwortmanager einloggen. Es ist der zentrale Schlüssel zu Ihren sämtlichen Passwörtern.

Geeignete Passwortmanager

Es gibt diverse Empfehlungen für sichere Passwörter: Das Bundesamt für Sicherheit und Informationstechnik (BSI) nennt den Passwortmanager Keepass als Empfehlung, die Stiftung Warentest hat im Juli-Heft 2022 einen Test zu geeigneten Passwortmanagern veröffentlicht und auch das Computer-Magazin chip.de hat im Mai 2022 einen Test durchgeführt. Das Ergebnis: Bei den kostenpflichtigen Angeboten schneiden die Softwareprogramme von 1Password, Enpass Individual, Bitwarden Premium und Dashline Premium laut chip.de sehr gut bis gut ab[2]. Bei Stiftung Warentest fanden sich 1Password, Dashlane Premium, Avira Password Manager (Pro) und Keeper Security Keeper Unlimited auf den vorderen Plätzen.[3]

Sie sollten sich ein wenig mit den Programmen beschäftigen, bevor Sie sich für eines entscheiden, das zu Ihren Ansprüchen passt. Finden Sie heraus, ob Ihnen zum Beispiel eine kostenlose Version genügt, wie etwa von Keepass oder auch eine Basisvariante von Bitwarden. Etwas ausgefeiltere Software bietet zum Beispiel eine Wiederherstellungsoption an, wenn Sie das Masterpasswort vergessen haben. Oder es wird mit der Zwei-Faktor-Authentifizierung gearbeitet, die zusätzliche Sicherheit bietet (siehe Abschnitt unten). Nicht zuletzt ist die Synchronisierung von mehreren Geräten meist nur bei den kostenpflichtigen Programmen möglich.



Bildquelle: artskill2k17 / Shutterstock.com

Tipp:

Die meisten Browser, etwa Firefox oder Chrome bieten an, sowohl Passwörter zu generieren oder auch abzuspeichern für die jeweilige Website. Das Passwort ist dann zumindest verschlüsselt für das jeweilige Gerät hinterlegt. Das ist besser als nichts, aber eine Spezial-Passwortmanager-Software bietet nach Ansicht von Experten mehr Sicherheit.

Alternative: Passwortliste anlegen

Sie sind vielleicht nicht so viel im Internet aktiv und haben gar nicht viele Nutzerkonten? Wenn Sie keinen Passwortmanager nutzen möchten – obwohl er auch bei wenigen Nutzerkonten und geringer Internetaktivität zu empfehlen ist – können Sie sich die Passwörter natürlich auch selbst ausdenken und archivieren. Aber bitte nicht auf dem PC als Datei speichern und auch nicht auf dem Smartphone! Wird Ihr PC gehackt oder Ihr Smartphone, etwa weil Sie sich einen Virus eingefangen haben, gelangen Kriminelle auch an Ihre Passwortdatei. Dann legen Sie lieber ganz klassisch mit Papier und Stift eine Passwortliste an und legen Sie diese an einem sicheren Ort ab. Das kann zum Beispiel ein Ort in Ihrer Wohnung sein, aber auch zum Beispiel ein Safe. Legen Sie die Liste im besten Fall auch noch einmal außerhalb Ihrer Wohnung ab, bei vertrauenswürdigen Freunden oder Familienmitgliedern. Es wäre nicht das erste Mal, dass Hochwasser oder ein Feuer persönliche Unterlagen vernichtet.

Bildquelle: photastic / Shutterstock.com

Lesetipp:

Hier erfahren Sie, wie Sie mit einem Notfallordner immer alle wichtigen Dokumente griffbereit haben: **https://www.biallo.de/soziales/news/notfallordner-wichtige-dokumente/**

So können Sie uns unterstützen

Wenn Ihnen unser ausführlicher und werbefreier Experten-Ratgeber gefallen hat, dann können Sie unser Team unterstützen, indem Sie als Wertschätzung eine Tasse Kaffee oder Tee spendieren.

PayPal:	**https://www.paypal.me/biallode/1,90**
Banküberweisung:	IBAN DE17 7009 1600 0002 5462 13
Stichwort:	RDW

Doppelte Sicherheit: Das bringt die Zwei-Faktor-Authentifizierung

Wenn Sie Online-Banking nutzen, dann nutzen Sie dort sicherlich auch die Zwei-Faktor-Authentifizierung: einen zusätzlichen Identifikationsprozess, um Ihre persönlichen Daten zu schützen. Sie geben dann Ihr Passwort ein, um sich bei Ihrem Onlinebanking anzumelden. Kommt es zu einem Überweisungsvorgang, müssen Sie zum Beispiel eine zusätzliche TAN-Nummer eingeben, die über eine separate App angezeigt wird oder ein Code wird Ihnen per SMS auf Ihr Handy geschickt, oder ein Fingerabdruck wird nötig oder ein Gesichtsscan – es gibt viele verschiedene Methoden.

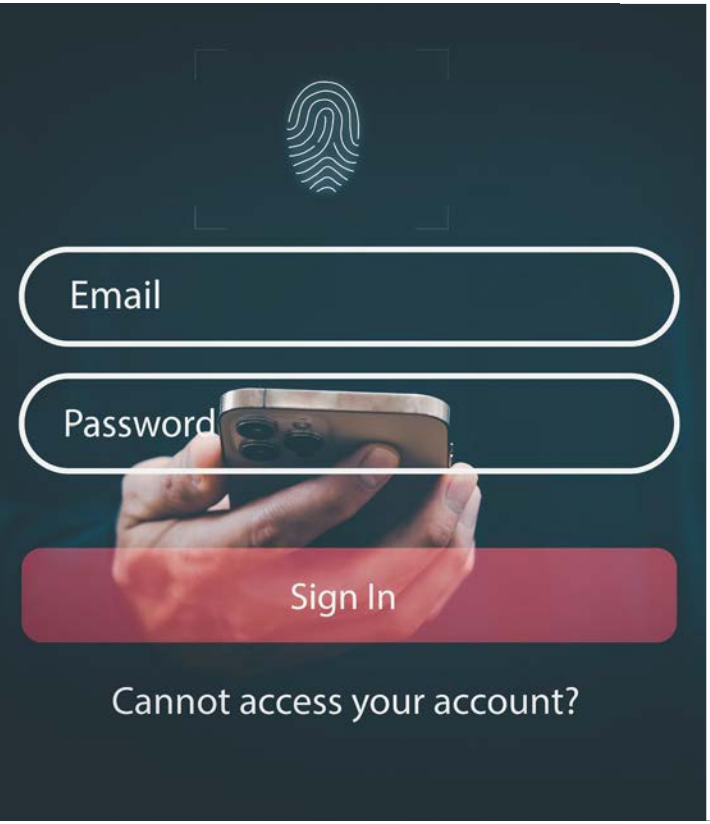
Diese Möglichkeit der zusätzlichen Identifizierung bieten inzwischen viele Online-Dienste an – Sie sollten sie unbedingt nutzen, weil sie ein Plus an Sicherheit bietet. Das gilt vor allem, wenn Sie bei einem Nutzerkonto Zahlungsinformationen hinterlegt haben. Auch Passwortmanager bieten zum Teil die Zwei-Faktor-Authentifizierung an, das erschwert noch einmal den Zugriff auf Ihre dort hinterlegten persönlichen Daten.

Bildquelle: Jirsak / Shutterstock.com

Passwort ändern: So gehen Sie vor

Wenn Ihre Passwörter nicht die Qualitätskriterien erfüllen, die wir in den vorherigen Abschnitten beschrieben haben, sollten Sie unbedingt handeln: Ändern Sie alle Passwörter, die nicht den Sicherheitsstandard erfüllen. Ja, das ist ein wenig Arbeit, aber sie lohnt sich. Der Vorteil ist, dass Sie sich die Arbeit nur einmal machen müssen, danach haben Sie ein standardisiertes Verfahren, mit dem Sie von da an immer vorgehen.

Bildquelle: Tapati Rinchumrus / Shutterstock.com



So ändern Sie Ihre Passwörter:

1. Laden Sie sich einen Passwortmanager auf Ihre Endgeräte.

2. Legen Sie eine Ordnerstruktur an, so dass Sie bei Bedarf Ihre dort abgelegten Passwörter schnell finden, zum Beispiel einen Ordner für alle Passwörter, die mit E-Mail-Konten zu tun haben, einen für Reisebuchungen, für Einkäufe, einen für alle Passwörter zu Softwareprogrammen und Online-Software-Abonnements et cetera.

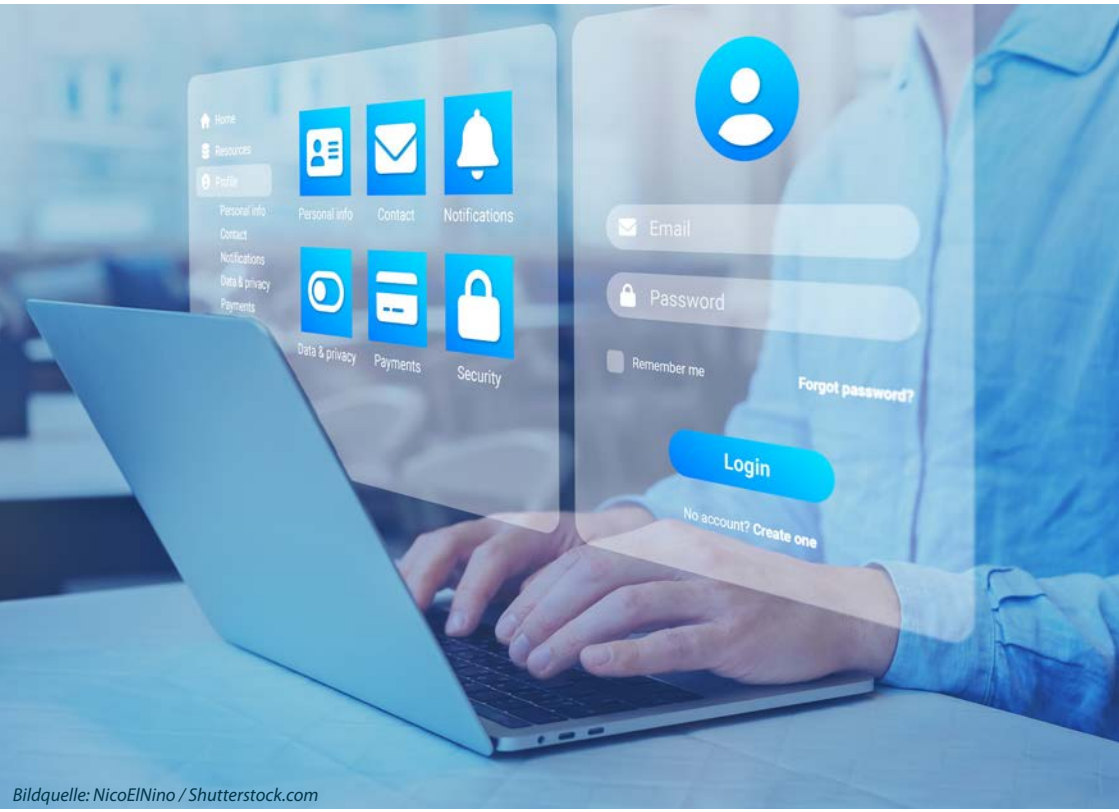
3. Wenn Sie beispielsweise das Passwort für ihr Amazon-Nutzerkonto ändern wollen, loggen Sie sich bei Ihrem Konto ein.

4. Gehen Sie dort auf „Mein Konto“ und dann „Anmelden und Sicherheit“. Hier können Sie Ihr Passwort ändern.

5. Öffnen Sie parallel dazu Ihren Passwortmanager und folgen dem Pfad, um ein neues Passwort anzulegen. Nach der Vergabe eines Namens für das neue Passwort (zum Beispiel Amazon) wird bei Keepass automatisch ein neues Passwort generiert. Kopieren Sie es und fügen Sie es in Ihrem geöffneten Amazon-Nutzerkonto als neues Passwort ein.

6. Amazon bietet die Zwei-Schritt-Verifizierung an, die der Zwei-Faktor-Authentifizierung entspricht. Aktivieren Sie diese ebenso! Dann wird Ihnen künftig ein Code per SMS auf das Handy geschickt, den Sie bei jeder Anmeldung dann zusätzlich eingeben. So ist Ihr Nutzerkonto maximal geschützt.
7. Wenn Sie sich künftig bei Amazon einloggen wollen, öffnen Sie parallel Ihren Passwortmanager und dort den Ordner, in dem Passwort für Amazon hinterlegt haben. Kopieren Sie es und geben Sie es bei Amazon als Passwort ein – fertig. Das dauert nur wenige Sekunden und bald haben Sie eine Routine entwickelt.

Gehen Sie mit der Methode alle Ihre Benutzerkonten durch und ändern Sie unsichere, schwache Passwörter. Ihr Passwort können Sie in den „Einstellungen" des Online-Dienstes ändern. Wenn Sie Zahlungsinformationen hinterlegt haben, dann sollten Sie auf jeden Fall auch die Zwei-Faktor-Identifizierung nutzen. Wird diese Variante nicht angeboten, sollten Sie den Online-Dienst nicht nutzen!



Bildquelle: NicoElNino / Shutterstock.com

Wenn das Passwort geknackt wurde: So gehen Sie bei einem Schaden vor

Ein erstes Indiz für ein geknacktes Nutzerkonto kann sein, dass Sie sich nicht mehr in ihr Konto einloggen können, trotz korrekter Passworteingabe und dass auch eine Passwort-Wiederherstellungsmail nicht bei Ihnen ankommt. Ebenso kann eine unbekannte Abbuchung auf dem Bankkonto ein Indiz dafür sein, dass Ihr Passwort geknackt wurde. Es kann aber ebenfalls sein, dass Sie eine E-Mail mit einer Zahlungsaufforderung eines Onlineshops erhalten. Das können auch Fake-Nachrichten sein, mit denen versucht wird, ihre Zugangsdaten abzugreifen (Phishing). Prüfen Sie die Mail deshalb genau, ob sie seriös ist: Stimmt der Absender? Stimmen Ihre Kundendaten? Sind alle Namen korrekt geschrieben? Auch wenn Sie zu der Annahme gelangen, dass die Mail seriös ist, klicken Sie auf keinen Link. Loggen Sie sich vielmehr auf der Homepage des Anbieters ein und überprüfen Sie, ob eine Bestellung dort hinterlegt ist. Sollte es sich wirklich um Betrug handeln, sollten Sie sofort handeln. Denn es wurde etwas in Ihrem Namen bestellt. Das heißt, Sie haften für die Bezahlung und auch für eventuelle Mahngebühren. Die Verbraucherzentrale hat gemeinsam mit dem Bundesinstitut für Sicherheit in der Informationstechnik (BSI) ein Vorgehen im Notfall erarbeitet und auf einer Notfallkarte zusammengetragen, die Sie in der Brieftasche mit sich tragen können.

Schritt 1: Informieren Sie den Anbieter des Onlineshops über den Vorfall.

Schritt 2: Kontaktieren Sie umgehend Ihre Bank und lassen Sie gegebenenfalls Ihre Kreditkarten sperren. Prüfen Sie, ob Sie bereits bezahlte Beträge zurückbuchen lassen können.

Schritt 3: Ändern Sie umgehend Ihr Passwort für den Shop-Account sowie Ihr E-Mail-Konto. Ändern Sie gegebenenfalls Passwörter anderer Online-Accounts. Nutzen Sie dasselbe Passwort nie für mehrere Accounts!

Schritt 4: Erstatten Sie Strafanzeige bei der Polizei. Sichern Sie Kontoumsätze und E-Mails als mögliche Beweismittel.

Quelle: BSI, Verbraucherzentrale

Bildquelle: wk1003mike / Shutterstock.com

Lesetipp:

Hier erfahren Sie, wie Sie Spam- und Phishing-E-Mails erkennen: **https://www.biallo.de/verbraucherschutz/ratgeber/spam-und-phishing-mails-erkennen/**

Quellenangaben:

[1]**HPI Identity Leak Checker:**
https://sec.hpi.de/ilc/

[2]**Computermagazin Chip.de (Passwortmanager):**
https://www.chip.de/artikel/Test-Die-besten-Passwort-Manager_182620837.html

[3]**Stiftung Warentest 7/2022: Butler und Bodyguard (Passwortmanager)**
Seite 34-39

Hasso-Plattner-Institut:
https://hpi.de/index.html

Verbraucherzentrale Rheinland-Pfalz:
https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672

https://www.verbraucherzentrale.de/sicher-im-internet-handy-tablet-und-pc-schuetzen-69691

Bundesamt für Sicherheit in der Informationstechnik (BSI):
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

Bundeskriminalamt:
https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110

Notfallkarte:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kampagne/Onlineshopping_SOS_Karte.pdf;jsessionid=3145ACFA3FB665B00B8C69792B3FC0DA.internet082?__blob=publicationFile&v=3#download=1

Bildquelle: Andrea Danti / Shutterstock.com

Impressum

Biallo & Team GmbH
Bahnhofstr. 25
Postfach 1148
86938 Schondorf

Telefon: 08192 93 379 - 0
Telefax: 08192 93 379 - 19
E-Mail: info@biallo.de
Internet: www.biallo.de

Vertretungsberechtigte Geschäftsführer: Horst Biallowons, Samuel Biallowons
Registergericht: Amtsgericht Augsburg
Registernummer: HRB 18274
Umsatzsteuer-Identifikationsnummer gemäß
§ 27 a Umsatzsteuergesetz: DE 213264656

Inhaltlich verantwortlich gemäß §§ 5 TMG, 55 RStV: Horst Biallowons

Das Impressum von biallo.de gilt auch für unsere Seiten auf

Youtube **Facebook** **Linkedin** **Twitter** **Instagram**