Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

3 Bilden Sie sichere Passwörter aus Sätzen
Passwörter müssen nicht kompliziert sein. Mit meiner Satz-Methode bauen Sie leicht zu merkende Passwörter.

4 Wort für Wort mehr Sicherheit
Beim Wort-Trick reihen Sie leicht zu merkende Begriffe aneinander: So klappt das Passwort-Merken garantiert!

6 In 1 Sekunde sicher bei Windows anmelden
Die Windows-Anmeldung per Fingerabdruckscanner ist besonders sicher und schnell. Windows öffnet nur für Sie!

7 Vergessen Sie nie mehr Ihre Passwörter
Verwenden Sie viele Passwörter? Legen Sie ein(e) Passwort-Buch oder -Liste als hilfreiche Gedächtnisstütze an.

+++ Sicherheitsfalle umgehen: Erstellen Sie mit meinen 7 Sicherheitsmethoden wirklich sichere Passwörter +++

13 Millionen Passwort-Hacks 2018: So schützen Sie sich

Am 3. Mai ist der Passwort-Tag, der PC-Anwender in aller Welt zu mehr Sicherheit ermahnen soll. Das ist bei Passwörtern dringend notwendig.

Jedes Jahr werden Millionen Konten gehackt, weil ihre Besitzer sehr einfache Passwörter wie **123456**, **123456789**, **1234**, **12345** oder **12345678** verwenden.

Das sind 5 der 10 häufigsten Passwörter deutscher PC-Anwender, die das Hasso-Plattner-Institut durch die Analyse gehackter Konten ermittelt hat. Geht es nach dem Institut sollen sichere Passwörter Buchstaben, Ziffern und Sonderzeichen enthalten und mindestens 15 Zeichen lang sein.

Unter den Top 1.000 der weltweit am meisten gehackten Passwörter ist nicht ein einziges sicheres Passwort. Stattdessen treffen Sie dort auf **computer**, **hellokitty**, **passwort** und **superman**.

Meine Empfehlung: Verwenden Sie ab sofort nur sichere Passwörter, die Sie nach meinen Vorgaben erstellen.

Viele Grüße, Ihr

Michael-Alexander Beisecker,
Deutschlands PC-Sicherheitsexperte Nr. 1

Lebenslange Sicherheit für Ihre Passwörter

7 Sicherheitsmethoden: So erstellen Sie wirklich unknackbare Passwörter

Ihre Passwörter sind die Schlüssel zum Zugang zu Ihrem PC, Ihrem E-Mail-Konto und Ihren anderen Online-Konten. Verwenden Sie für alle Ihre Konten dasselbe Passwort, braucht ein Hacker nur diesen einen Schlüssel und hat Zugriff auf alle Ihre gespeicherten Daten. Um Sie vor dieser Sicherheits-Falle zu schützen, zeige ich Ihnen anhand meiner einzigartigen Passwort-Methode, wie Sie sichere Passwörter erstellen, die Sie sich zudem einfach merken können.

Je schwieriger Ihre Passwörter zu knacken sind, umso sicherer sind Ihre wichtigen Daten. Das ist wie bei Ihrer Haustür: Kann ein Einbrecher das Schloss nicht innerhalb weniger Minuten überwinden, gibt er meist auf. Es kommt also darauf an, sichere Passwörter zu finden und keinen „Generalschlüssel“ zu verwenden.

Mein wichtigster Sicherheitstipp lautet daher: Setzen Sie für jedes Ihrer Online-Konten ein eigenes Passwort ein. Die Frage ist nur: Wie merken Sie sich so viele Passwörter und wie wirksam schützen Sie mit diesen Passwörtern Ihre Daten?

Meine 7 Sicherheitsmethoden: So erstellen Sie einbruchssichere Passwörter und eine sichere Passwort-Liste

Methode 1:	Versetzen Sie sich in die Denkmuster eines Hackers (siehe Seite 2).
Methode 2:	Erzeugen Sie mit dem Satz-Trick Passwörter aus Wörtern, Ziffern und Sonderzeichen (siehe Seite 3).
Methode 3:	Beim Wort-Trick reihen Sie einfach mehrere leicht zu merkende Wörter aneinander (siehe Seite 4).
Methode 4:	Variieren Sie die Satz- und die Wort-Methode für sichere Passwörter (siehe Seite 5).
Methode 5:	Melden Sie sich in 1 Sekunde per PIN oder Fingerabdruckscanner an Ihrem Windows-PC an (siehe Seite 6).
Methode 6:	Dank unknackbarer Passwort-Liste oder Passwort-Buch verlieren Sie nie mehr ein Passwort (siehe Seite 7).
Methode 7:	Überprüfen Sie Ihre neuen Passwörter: Sind sie wirklich sicher? (siehe Seite 8).

Diese 7 Methoden bauen aufeinander auf. Wenden Sie daher alle Methoden bei Ihren Passwörtern an, um garantiert sicher zu sein.

>>> Lesen Sie bitte weiter auf Seite 2

>>> Fortsetzung von Seite 1

Methode 1: Versetzen Sie sich in die Denkmuster eines Hackers und erkennen Sie die Passwort-Fallen

Viele PC-Anwender verwenden zu kurze und sehr einfache Passwörter wie 12345678. Dieses eine, leicht zu hackende Passwort wird dann auch noch mehrfach eingesetzt und zur Absicherung aller Online-Konten verwendet. Hacker knacken solche einfachen Passwörter in wenigen Sekunden. Damit Sie nicht in diese Falle tappen, zeige ich Ihnen in diesem Beitrag, wie Hacker an Ihre Passwörter gelangen und wie Sie sich wirksam davor schützen.

Schon der Zugriff auf ein E-Mail- oder Multimedia-Konto reicht, um einen Domino-Effekt auszulösen: Innerhalb weniger Minuten, maximal Stunden ist ein Hacker im Besitz aller Ihrer Online-Konten. Häufig werden dann Betrugs-Mails unter Ihrem Namen versendet, es werden auf Ihren Namen Waren bestellt oder die Kriminellen übernehmen Ihre Identität für andere Straftaten.

Die 7 Denkmuster der Hacker und wie Sie die Angriffe abwehren

Hacker-Denkmuster 1: Hacken Ihres Kontos durch Ausprobieren (Brute-Force-Methode)

Die meisten Konten-Hacks erfolgen mithilfe spezieller Tools, die umfangreiche Passwort-Tabellen enthalten. Das Tool führt eine automatische Anmeldung bei Ihrem Konto durch und probiert nacheinander alle Tabelleneinträge aus. Bei einfachen Passwörtern reichen dazu wenige Versuche und das Konto ist gehackt.

Ihr Schutz: Verwenden Sie in Ihren Passwörtern keine persönlichen Informationen wie Namen, Geburtsdaten oder Interessen. Je länger Ihr Passwort ist, umso sicherer ist es. Bei einem zum Beispiel 30-stelligen Passwort bräuchte ein aktueller PC mehrere Millionen Jahre, um alle Kombinationen auszuprobieren.

Hacker-Denkmuster 2: Hacken Ihres Kontos über die persönliche Frage

Viele Konten bieten eine Passwort-Wiederherstellungsfunktion. Haben Sie das Passwort vergessen, wird Ihnen eine persönliche Frage gestellt, wie z. B.: „Wie lautet der Name Ihrer Mutter?“, oder: „Wie lautet der Name Ihres Haustiers?“ Hat ein Hacker persönliche Informationen über Sie, kann er diese Fragen auch beantworten und somit auf Ihr Konto zugreifen.

Ihr Schutz: Überprüfen Sie die eingestellten Fragen und Antworten bei Ihren Konten. Sie können falsche Antworten hinterlegen, um Hacker in die Irre zu führen. Oder Sie tragen als Antwort ein zweites, sicheres Passwort ein.

Hacker-Denkmuster 3: Hacken Ihres Kontos mit der „Passwort vergessen“-Methode

Erhält ein Hacker die Kontrolle über eines Ihrer E-Mail-Konten, das als zweite Kontaktmöglichkeit (Referenzkonto) angegeben ist, kann er bei einem Ihrer anderen Online-Konten einfach auf **Passwort vergessen** klicken und erhält eine E-Mail mit einer Anleitung, wie er das Passwort Ihres anderen Kontos ändern kann. Sie sind dann ausgesperrt!

Ihr Schutz: Ein sicheres Passwort allein schützt Sie bei einem Online-Konto nicht zuverlässig genug, wenn Sie mobil mit Notebook, Tablet oder Smartphone Ihre E-Mails abfragen. Stiehlt jemand Ihr Mobilgerät und es ist nicht ausreichend gegen unbefugten Zugriff geschützt, kann der Dieb auf Ihr auf diesem Gerät eingerichtetes E-Mail-Konto zugreifen. Schützen Sie Windows daher immer mit einem sicheren Passwort und aktivieren Sie bei Ihrem Smartphone die PIN-Sperre in den Einstellungen.

Hacker-Denkmuster 4: Hacken Ihrer Konten über einen „Universalschlüssel“

Hat ein Hacker Zugriff auf Ihr Facebook-, Google-, Microsoft- oder Twitter-Konto, kann er sich darüber bei vielen anderen Diensten anmelden. Solche Konten ermöglichen den Zugriff auf verschiedenste Dienste, im Fall von Microsoft zum Beispiel auf Windows, OneDrive (Online-Speicher), Outlook.com (E-Mail) oder Skype.

Ihr Schutz: Seien Sie sich dieser Gefahr bewusst und vergeben Sie für Windows (Microsoft-Konto), Ihr Android-Smartphone (Google-Konto) und Social-Media-Dienste wie Facebook und Twitter besonders sichere Passwörter. Ändern Sie das betreffende Passwort sofort, wenn Sie den Verdacht auf einen Missbrauch des entsprechenden Kontos haben.

Hacker-Denkmuster 5: Ausspähen Ihrer Passwörter über Schadprogramme

Hacker verwenden Spionageprogramme, die Ihre Tastatureingaben kopieren (Keylogger), Bildschirmkopien erstellen, Ihre Daten durchsuchen oder über Ihre Webcam Ihre Tastatureingaben mitlesen. Darüber finden die Hacker heraus, welche Dienste Sie verwenden und welche Passwörter.

Ihr Schutz: Öffnen Sie keine E-Mail-Anhänge von unbekannten Absendern. Laden Sie nur die von mir empfohlenen Programme. Verwenden Sie ein aktuelles Windows 10 oder 7 und nur aktuelle Programme, die vom Hersteller noch gepflegt werden, um z. B. Sicherheitslücken zu schließen.

Hacker-Denkmuster 6: Ausspähen Ihrer Passwörter über Betrugsseiten

Insbesondere beim Online-Banking finden Hacker die Passwörter vor allem über Betrugsseiten heraus. Dazu werden gefälschte E-Mails versendet, die kaum von denen Ihrer Hausbank zu unterscheiden sind. Darin werden Sie aufge-

fordert, auf einen Link zu klicken und Ihre Zugangsdaten auf der vermeintlichen Bankseite einzugeben.

Ihr Schutz: Seien Sie bei angeblichen Bank-Mails äußerst misstrauisch und klicken Sie auf keinen Fall auf einen Link darin. Geben Sie die Adresse der Webseite Ihrer Hausbank immer persönlich in den Browser ein, wenn Sie darauf zugreifen möchten.

Hacker-Denkmuster 7: Hacken Ihrer Geräte-Konten über die Voreinstellung

Zum Hacken eines Großteils von Routern, Webcams und anderen internetfähigen Geräten braucht ein Hacker nur die Gerätebezeichnung zu kennen. Er probiert dann einfach das einheitlich voreingestellte Administrator-Passwort aus und hat damit in vielen Fällen Glück. Danach kommt wieder der Domino-Effekt ins Spiel, denn über einen gehackten Router kann ein Hacker Ihren PC manipulieren oder Sie über eine Webcam ausspionieren.

Ihr Schutz: Überprüfen Sie bei jedem angeschlossenen Gerät, ob es einen Passwort-Schutz hat und ob Sie das voreingestellte Passwort geändert haben. Wichtig ist das vor allem bei Routern, Webcams und Smart-Home-Geräten wie Heizungsreglern, einer Lichtsteuerung oder auch einem internetfähigen Fernseher (Smart TV).

Verwenden Sie sichere Passwörter, kann ein Hacker diese nicht durch Ausprobieren herausfinden, es würde schlicht zu lange dauern. Vollkommen sicher vor Konten-Hacks sind Sie aber nur, wenn Sie bei allen Ihren Konten und Geräten sichere Passwörter verwenden und sich nicht durch Schadprogramme und Betrugs-Seiten ausspionieren lassen.

Tappen Sie nicht in diese 3 Gedankenfallen

- **Hacker interessieren sich nicht für mich:** In den Medien lesen Sie viel über gehackte Prominente, Industriespionage und hohe Schäden beim Online-Banking-Betrug. Die meisten Menschen denken dann: „Ich bin nicht prominent, kein Geheimnisträger und auch nicht reich, mir kann nichts passieren."

  Die Gefahr: Sie fühlen sich sicher, achten nicht genug auf Ihre Passwörter und werden wie Millionen andere PC-Anwender gehackt. Es geht nicht um Ihre Person, sondern um die Sicherheit Ihrer Passwörter und damit um Ihre Konten.
- **Meine Daten sind nicht so wichtig:** Häufig wird auch die Wichtigkeit der Daten in den Vordergrund gerückt. So sind etwa das Online-Banking-Konto und die Konten bei Online-Shops gut abgesichert, aber bei weniger wichtig erscheinenden Konten wird ein Einheits-Passwort verwendet – und zwar ein und dasselbe Passwort über Jahrzehnte.

  Die Gefahr: Es kommt bei einem Konto nicht immer auf die Daten an. Ein gehacktes Konto ist häufig der Einstieg für weitere Hacks, die unter „Die 7 Denkmuster der Hacker" beschrieben sind (Seite 2).
- **Ich verwende sichere Passwörter, mir kann nichts passieren:** Es ist sehr gut, dass Sie zu den sicherheitsbewussten PC-Anwendern gehören und auf Ihre Passwörter achten. Das schützt Sie, aber das reicht nicht.

  Die Gefahr: Hacker haben Methoden, um auch sichere Passwörter zu ermitteln, wie Sie im Folgenden lesen.

Ihr Schutz: So kommen Hacker nicht an Ihre Passwörter

Öffnen Sie keine E-Mail-Anhänge und andere fremde Dateien ohne Prüfung. Installieren Sie auch keine unbekannten Programme. Nur wenn Sie diese Maßnahmen beherzigen, sind Sie mit sicheren Passwörtern bestmöglich geschützt.

Methode 2: Erzeugen Sie mit dem Satz-Trick Passwörter aus Wörtern, Ziffern und Sonderzeichen

Sichere Passwörter sind mindestens 15 Zeichen lang, enthalten Klein- und Großbuchstaben, Ziffern und Sonderzeichen. Doch wie kommen Sie auf einfache Weise zu solchen Passwörtern, die sich dann auch noch einfach merken lassen? Eine Methode ist der Satz-Trick. Damit erzeugte Passwörter lassen sich nicht nur supereinfach merken, sondern auch gefahrlos aufschreiben.

Denken Sie sich einen längeren Satz aus, der für Sie einfach zu merken ist. Das klappt besonders gut, wenn Sie im Satz etwas beschreiben, das Sie gerne und regelmäßig tun, wie Fernsehen schauen oder essen.

LESERSERVICE

Redaktionshilfe: Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter **https://club.computerwissen.de** an und stellen Sie ihm dort Ihre Fragen. **Michael-Alexander Beisecker** und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

Sie können zum Beispiel Sätze verwenden wie: „Abends schaue ich im ZDF immer um 19:00 Uhr die Heute-Sendung.“ Oder: „Sonntags gibt es bei uns immer um 13:00 Uhr Mittagessen.“ Oder: „Durch die neuen LED-Lampen im Wohnzimmer spare ich pro Jahr 13,48 EUR.“

In nur 2 Schritten wandeln Sie Ihren Satz in ein sicheres Passwort um

So verwandeln Sie zum Beispiel den Satz „**J**eden **S**onntag **g**ehe **i**ch **u**m **15:00 U**hr **i**m **W**ald **s**pazieren.“ in ein sicheres Passwort:

1. Zählen Sie die Wörter, Ziffern und Sonderzeichen im Satz. Die Summe sollte mindestens 15 sein. Der Beispielsatz hat 9 Wörter, 4 Ziffern (1, 5, 0, 0) und 2 Sonderzeichen, nämlich den Doppelpunkt bei der Uhrzeitangabe und einen Satzendepunkt. Die Summe ist 15.
2. Schreiben Sie nun die Anfangsbuchstaben der Wörter, die Ziffern und Sonderzeichen hintereinander auf. Sie bilden Ihr neues Passwort. Im Beispiel lautet es **JSgiu15:00UiWs**. und hat die Mindestlänge von 15 Zeichen.

Wie Sie die Sicherheit beim Satz-Trick erhöhen

Verräterische Uhrzeit: Ein Hacker wird ein Passwort wie **JSgiu15:00UiWs.** im Normalfall nicht hacken. Analysiert ein Hacker aber mehrere Passwörter dieser Art, wird er schnell erkennen, dass **15:00U** für eine Uhrzeit steht.

Ihre Lösung: Machen Sie die Uhrzeit weniger kenntlich, indem Sie zum Beispiel das U weglassen, nur die erste Ziffer verwenden und statt des Doppelpunktes ein anderes Zeichen einsetzen wie etwa ein ° oder ^. Das Ergebnis ist **JSgiu1°iWs.** oder **JSgiu1^iWs.**. Mit 11 Zeichen wären diese Beispiel-Passwörter allerdings zu kurz. Sie müssten also den Satz verlängern, einen anderen Satz wählen oder Zeichen ergänzen.

Wiederholtes Satzendezeichen: Am Ende eines Passworts steht beim Satz-Trick immer ein Satzendezeichen, also ein Punkt oder Ausrufezeichen. Das könnte als Regel in ein Hacker-Programm aufgenommen werden und solche Passwörter wären somit erheblich schneller zu hacken.

Ihre Lösung: Lassen Sie das Satzendezeichen weg, setzen Sie es an den Anfang des Passworts oder ersetzen Sie es durch ein ganz anderes Zeichen. Das Ergebnis sind Passwörter wie **JSgiu15:00UiWs** (ohne Punkt), **.JSgiu15:00UiWs** (Punkt am Satzanfang) oder **JSgiu15:00UiWs{** (geschweifte offene Klammer statt Satzendezeichen).

Geringe Zahl an Sonderzeichen: In Sätzen dieser Art kommt zudem nur eine beschränkte Anzahl an Sonderzeichen wie Ausrufezeichen (!), Punkt (.), Komma (,), Doppelpunkt (:) und Bindestrich (-) vor.

Ihre Lösung: Fügen Sie Sonderzeichen hinzu, überlegen Sie sich Sätze mit anderen Sonderzeichen oder ersetzen Sie häufig vorkommende Sonderzeichen durch andere. Seien Sie kreativ!

Wie Sie aus dem Satz-Trick eine hackersichere Methode machen

Der Satz-Trick bietet deutlich mehr Sicherheit als ein Passwort wie **123456789**. Es besteht jedoch die Gefahr auffälliger Wiederholungen, wie bei Uhrzeiten oder immer gleichen Satzanfängen.

Erkennt ein Hacker aus Ihrem Umfeld den Satz-Trick, schützt das betreffende Passwort nicht mehr gut. Weiß Ihr Nachbar zum Beispiel, dass Sie jeden Sonntag um 15:00 Uhr im Wald spazieren gehen, kann er das Beispiel-Passwort **JSgiu15:00UiWs.** durchaus erraten.

Kombinieren Sie den Satz-Trick daher mit dem nachfolgenden Wort-Trick (Methode 3, unten auf dieser Seite).

Meine Empfehlung: Verwenden Sie für den Satz-Trick keine Bibelzitate, zumindest nicht in der Originalversion. Tabu sind auch berühmte Filmzitate wie: „Der Unterschied zwischen Wahnsinn und Genie definiert sich lediglich aus dem Erfolg.“ („Der Morgen stirbt nie“, James-Bond-Film von 1997). Passwort-Knacker-Tools enthalten solche Zitate in ihren Wörterbüchern.

Methode 3: Beim Wort-Trick reihen Sie einfach mehrere leicht zu merkende Wörter aneinander

Dass ein Passwort wie „aS8%4,&xN9?14Oqj.1!“ sicher ist, leuchtet auf Anhieb ein. Genauso sicher ist aber auch ein Zufallsreim wie „A human visitor despised ensuring Aero theorized.“ Das Hacken eines solchen Passwortes würde mit aktuellen PCs 5 Millionen Jahre dauern (Quelle: „How to Memorize a Random 60-Bit String“, University of Southern California). Sie brauchen jedoch kein Englisch zu lernen oder Dichter zu werden. Es reicht, wenn Sie ein paar deutsche Wörter aneinanderreihen, wie zum Beispiel „einfach Pferd Batterie Büroklammer Magnet“ (Quelle: Universität Weimar, Crypto-Party). Schon ist Ihr sicheres Passwort fertig!

Die Sicherheit beim Wort-Trick liegt in der Länge des Passworts. Nur deshalb werden die Passwörter nicht gehackt, obwohl nur Klein- und Großbuchstaben verwendet werden und alle Wörter in den Wörterbüchern der Hacker-Tools enthalten sind. Im Grunde reichen beim Wort-Trick schon drei bis vier Wörter, die Sie aneinanderreihen, für

ein sicheres Passwort aus, etwa **Kirsche**, **Kraftwagen** und **Berliner**.

Wichtig: Beachten Sie diese 4 Sicherheitsregeln

1. Achten Sie darauf, dass die Wörter aus unterschiedlichen Fachgebieten stammen und nicht etwa alle mit Ihrer Arbeit oder Ihren Hobbys in Verbindung stehen.

Mein Tipp: Die Wörter **hacken Melissa Trojaner** sind ungeeignet, da sie alle aus dem Bereich PC-Sicherheit stammen. Das ist bei **Kirsche**, **Kraftwagen** und **Berliner** nicht der Fall.

2. Verwenden Sie keine Namen von Freunden oder Familienmitgliedern, wie zum Beispiel bei **Klaus Anja Sebastian**. Das könnte jemand aus Ihrem Umfeld zu leicht erraten.
3. Setzen Sie keine Wortkombinationen ein, die in einem logischen Zusammenhang stehen, z. B. **Berliner** und **Weiße** (das Getränk Berliner Weiße) oder **Stuhl** und **Bein** (Stuhlbein).
4. Keines der Wörter darf sich wiederholen, die Wortkombination **Affe Banane Banane** ist also in doppelter Weise ungeeignet, da das Wort **Banane** zweimal verwendet wird und zudem noch ein logischer Zusammenhang zu **Affe** besteht.

In 3 Schritten zu einem sicheren und kurzen Passwort

Ist Ihnen die Eingabe der kompletten Wörter zu mühsam, kombinieren Sie den Wort-Trick mit dem Satz-Trick: Sie erhalten ein kurzes, sicheres und dennoch leicht zu merkendes Passwort:

1. Wählen Sie zunächst einige Wörter aus, die Sie für Ihr Passwort verwenden möchten. Achten Sie dabei auf die vier nebenstehenden Sicherheitsregeln.
2. Bilden Sie aus den Wörtern einen Satz. Im Fall von **Kirsche**, **Kraftwagen** und **Berliner** wäre das etwa: „Die Kirschen im Berliner Kraftwagen wurden um 16:00 Uhr geliefert."
3. Wandeln Sie nun den Satz in ein Passwort um, wobei Sie die Anleitung aus Methode 2 verwenden. Das Ergebnis wäre zum Beispiel **DKiBKwu16:00Ug.**.

Meine Empfehlung: Notieren Sie sich Ihre Passwörter in einer unknackbaren Passwort-Liste oder einem Passwort-Buch (siehe Seite 7).

Methode 4: Variieren Sie die Satz- und Wort-Methode für sichere Passwörter

Laut dem Bundesamt für die Sicherheit in der Informationstechnik verwenden 81 Prozent der deutschen Internet-Nutzer ein Passwort für mehrere oder alle genutzten Online-Dienste. Das ist auch bei einem sicheren Passwort extrem gefährlich. Gelangt ein Hacker auch nur bei einem von Ihnen genutzten Dienst in den Besitz des Passwortes, kann er damit auch auf alle anderen von Ihnen genutzten Dienste zugreifen. Ist dem Hacker nicht bekannt, welche Online-Dienste Sie verwenden, meldet er sich einfach testweise bei allen bekannten Diensten mit Ihrem Benutzernamen und Passwort an. Mit meiner Sicherheitsmethode 4 umgehen Sie diese Passwort-Falle gekonnt.

Heute verwendet jeder zweite Internet-Nutzer 10 oder mehr Internet-Dienste und entsprechend viele Passwörter. Es ist lästig, alle diese Passwörter aufzuschreiben und die Passwort-Liste immer wieder zu pflegen. Der Ausweg: Sie verwenden ein sicheres Grund-Passwort und erweitern es bei jedem Anbieter um ein paar Zeichen.

Wie Sie einfach zu unterschiedlichen Passwörtern kommen

Nehmen wir zum Beispiel das Passwort **KirscheKraftwagenBerliner**, das Beispiel aus dem Wort-Trick (siehe Methode 3, Seite 4). Sie könnten es für alle Ihre Dienste verwenden, wenn Sie jeweils noch etwas davorsetzen oder anhängen.

Üblicherweise werden zur Variation die ersten Zeichen des Anbieternamens verwendet. Sehen Sie sich das Beispiel in der folgenden Tabelle an:

Anbieter	Erste 3 Zeichen	Passwort
Amazon	Ama	KirscheKraftwagenBerliner**Ama**
eBay	eBa	KirscheKraftwagenBerliner**eBa**
Computerwissen Club	Com	KirscheKraftwagenBerliner**Com**
Facebook	Fac	KirscheKraftwagenBerliner**Fac**
Windows	Win	KirscheKraftwagenBerliner**Win**

Ein Grund-Passwort für fünf Dienste lässt sich leichter merken als fünf verschiedene Passwörter.

Vorsicht: Passwort-Variationen verbergen ein Risiko

Gelangt ein Hacker – auf welchem Wege auch immer – in den Besitz von zwei oder mehr Ihrer Passwörter, analysiert er Ihre Passwörter womöglich.

Da sich die Passwörter nur in den letzten Stellen unterscheiden, ist die Variation sofort ersichtlich. Das Erraten

der restlichen Passwörter fällt dann nicht schwer, egal, wie sicher diese sonst konstruiert wurden.

Überlegen Sie sich daher ein nicht so leicht erkennbares Muster. Fügen Sie zum Beispiel die drei Buchstaben nach jedem Wort Ihres Grund-Passwortes ein, lautet es im Fall von Amazon statt KirscheKraftwagenBerliner**Ama** nun Kirsche**A**Kraftwagen**m**Berliner**a**.

Meine Empfehlung: Die Sicherheit der Passwörter, die Sie über die Variationen gebildet haben, ist nur für die private Verwendung ausreichend. Für die Passwörter in einem Unternehmen empfehle ich diese Methode nicht, denn hier ist die Gefahr, dass Passwörter durch Unbefugte analysiert werden, höher als beim privaten Einsatz.

Methode 5: Melden Sie sich in 1 Sekunde per PIN oder Fingerabdruckscanner an Ihrem Windows-PC an

Das wichtigste Passwort ist das Windows-Kennwort. Hat jemand Zugang zu Ihrem PC, kann er damit praktisch auf alle Ihre Daten zugreifen. Nur ein langes, sicheres Windows-Kennwort schützt Sie vor dieser Gefahr. Doch dieses Passwort müssen Sie mehrfach am Tag eingeben. Das ist lästig und zeitraubend. Der sichere Ausweg ist eine PIN oder ein Fingerabdruckscanner. Das erspart Ihnen die mehrmalige Passwort-Eingabe am Tag. Eine PIN oder einen Fingerabdruckscanner einzurichten, ist bei Windows 10 ganz einfach.

Zur Vergabe einer PIN (**P**ersönliche **I**dentifikations **N**ummer) rufen Sie die Einstellungen Ihres Windows 10 auf:

1. Öffnen Sie das **Start**-Menü und über das **Zahnrad**-Symbol die **Einstellungen**.
2. Wählen Sie **Konten** und links das Register **Anmeldeoptionen**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie Ihr sicheres Windows-Kennwort ein.
5. Tippen Sie Ihre PIN ein. Sie kann allein aus Ziffern bestehen oder nach dem Aktivieren der Option **Buchstaben und Symbole einschließen** auch andere Zeichen enthalten. Ihre PIN sollte wie bei Ihrer EC-Karte mindestens 4 Ziffern lang sein.
6. Klicken Sie auf **OK**.
7. Melden Sie sich von Windows ab und erneut an. Sie werden jetzt nach der PIN statt nach Ihrem Kennwort gefragt.

Wie bei einem Passwort müssen Sie natürlich auch die PIN immer zur Hand haben und sich gut merken können. Suchen Sie nach einem sicheren Windows-Zugang, ohne sich eine Kennung merken zu müssen, empfehle ich Ihnen einen Fingerabdruckscanner. Die Geräte sind nicht teuer und nehmen Sie in wenigen Minuten in Betrieb – überzeugen Sie sich in folgender Anleitung.

Nie mehr zur Anmeldung tippen: Fingerabdruckscanner bei Windows 10 einrichten

Ich selbst verwende statt einer PIN den schnellsten Fingerabdruckscanner der Welt: „My Lockey“ der Firma PQI scannt Ihren Fingerabdruck in 0,15 Sekunden und kostet rund 30 €.

Das Einrichten eines Fingerabdruckscanners erfordert höchstens 5 Minuten – so geht‘s:

1. Stecken Sie den Fingerabdruckscanner an eine freie USB-Buchse Ihres PCs. Ist Ihre Tastatur oder Ihr Flachbildschirm mit einem USB-Anschluss ausgestattet, können Sie den Fingerabdruckscanner auch daran anschließen.

Mein Tipp: Achten Sie darauf, dass Sie den Scanner leicht nutzen können. Stellen Sie ihn hierfür an einem gut erreichbaren Platz auf, wie z. B. neben die Tastatur. Wählen Sie bei einem Desktop-PC eine Buchse an der Frontseite oder schließen Sie den Scanner über ein USB-Verlängerungskabel an der Rückseite an.

2. Windows erkennt den Fingerabdruckscanner automatisch und richtet ihn sofort ein. Sie erhalten dabei ein akustisches Signal, aber keine Meldung.
3. Öffnen Sie das **Start**-Menü ⊞ und klicken Sie auf das **Zahnrad**-Symbol ⚙ zum Aufrufen der **Einstellungen**.
4. Wählen Sie **Konten** und öffnen Sie links das Register **Anmeldeoptionen**.
5. Klicken Sie unterhalb von **Fingerabdruck** auf die graue Schaltfläche **Einrichten**.
6. Sie werden von Windows Hello begrüßt. Klicken Sie auf **Los geht’s** und folgen Sie dem Assistenten. Sofern Sie dazu aufgefordert werden, geben Sie die PIN und/oder das Kennwort zu Ihrem Windows-Konto ein.
7. Berühren Sie den Fingerabdruckscanner mit einem Ihrer Finger, wenn Sie dazu aufgefordert werden. Wahlweise können Sie über **Weitere Finger hinzufügen** noch weitere Fingerabdrücke scannen, um sich alternativ mit einem anderen Finger anmelden zu können oder

mehreren Personen den Zugang zum betreffenden Konto zu gestatten. Vergessen Sie nicht, das Fenster zu schließen.

Den Fingerabdruckscanner können Sie für mehrere Geräte verwenden, also zum Beispiel zu Hause am Desktop-PC und unterwegs am Notebook.

Meine Empfehlung: Wenn Ihnen die Kosten von rund 30 € für den blitzschnellen Fingerabdruckscanner nicht zu hoch sind, empfehle ich Ihnen diese Methode. Sie werden die Anmeldung per Fingerabdruckscanner nicht mehr missen wollen. Zum Anmelden tippen Sie nur noch einmal mit dem entsprechenden Finger auf den Fingerabdruckscanner oder ziehen ihn darüber und sind in weniger als 1 Sekunde sicher angemeldet.

Methode 6: Dank unknackbarer Passwort-Liste oder Passwort-Buch verlieren Sie nie mehr ein Passwort

Sie haben mit den Methoden 2 bis 4 Ihre sicheren Passwörter gefunden. Sichere Passwörter sind nicht einfach zu merken. Schreiben Sie Ihre Passwörter daher auf, um Sie bei Bedarf nachzuschlagen. Ich empfehle Ihnen hier eine einfache Lösung. Ein Blatt Papier und ein Stift reichen dafür aus. Sie sollten jedoch ein paar Sicherheitsregeln beachten, damit Ihre Passwort-Liste nicht von unbefugten Personen missbraucht werden kann. Haben Sie eine größere Menge Passwörter ist ein Passwort-Buch die beste Form der Aufbewahrung.

Die 4 schlimmsten Fehler im Umgang mit Passwort-Listen

Herkömmliche Passwort-Listen, Passwort-Bücher oder Notizzettel mit Passwörtern sind sicher, wenn sie im Tresor liegen oder sicher versteckt sind. Stattdessen sehe ich aber immer wieder diese vier schlimmen Fehler:

1. Passwörter werden auf einer Haftnotiz notiert und direkt sichtbar auf den Bildschirm geklebt.
2. Die Liste der Passwörter liegt griffbereit unter der Tastatur, unter der Schreibtischunterlage oder in einer Schublade des Schreibtischs.
3. Alle Passwörter sind im Terminkalender eingetragen, der auf dem Schreibtisch liegt.
4. Der schlimmste Fehler: Die Passwörter werden in eine Textdatei oder Tabelle geschrieben und auf dem PC gespeichert. Ein Schadprogramm wird sie dort sicher finden.

Ihre Passwörter haben Sie bei diesen bequemen Ablagen zwar immer zur Hand, aber auch jeder Besucher und Einbrecher kann die Passwörter sofort finden und nutzen.

Die sichere Passwort-Liste: So sind Ihre Passwörter unerkennbar und ohne Hilfsmittel nicht zu nutzen

Eine sichere Passwort-Liste können Sie dagegen direkt am PC liegen lassen. Sie müssen diese nur so gestalten, dass ein Nichteingeweihter damit nicht zurechtkommt:

1. Haben Sie Ihre Passwörter mit der Satz-Methode (siehe Seite 3) gebildet, schreiben Sie die Sätze auf und lassen den Zettel wie einen normalen Notizzettel aussehen. Dazu bilden Sie Sätze wie in einer Aufgaben- oder Einkaufsliste.

Aufgaben	Daraus abgeleitetes Satz-Passwort
Montag ab 17 Uhr den Anzug aus der Reinigung abholen, kostet ca. 15 €.	Ma17UdAadRa,kc.15€

Beispiel für einen Eintrag einer geheimen Passwort-Liste.

2. Nutzen Sie die Wort-Methode (siehe Seite 4), schreiben Sie ebenfalls Sätze mit den verwendeten Wörtern.

Aufgaben	Daraus abgeleitetes Wort-Passwort
Bügeleisen für Reise nach Australien bei eBay kaufen.	**BügeleisenReiseAustralien** eBay ist Ihr Hinweis darauf, für welchen Dienst dieses Passwort verwendet wird.

Beispiel für einen Eintrag einer geheimen Passwort-Liste mit Hinweis auf das jeweilige Online-Konto.

3. Verwenden Sie die Variationen-Methode (siehe Seite 5), schreiben Sie irgendwo möglichst unauffällig das Grund-Passwort am Arbeitsplatz auf. Das ist alles, was Sie benötigen, denn die Variationen bilden Sie über die Namen der jeweiligen Dienste.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299

Dieses monothematische Supplement „Hackerschutz durch sichere Passwörter" gehört zu dem Titel „Ihr PC-Sicherheits-Berater".

Computerwissen, ein Verlagsbereich der VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop

Chefredakteur: Michael-Alexander Beisecker (V.i.S.d.P.), Oberhausen

Herausgeberin: Patricia Sparacio

Adresse: Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2-4, 53177 Bonn

Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165

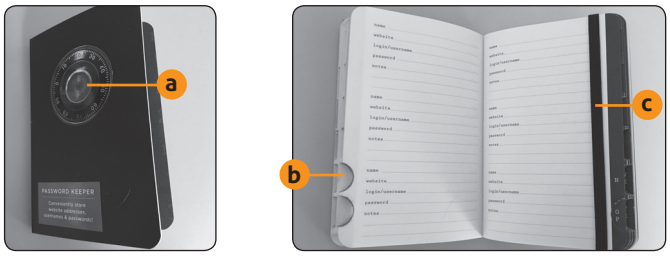
Ihre Alternative zur Passwort-Liste: Das Passwort-Buch

In der Praxis haben Passwort-Listen jedoch meist zwei Nachteile: Es passen nicht alle verwendeten Passwörter hinein und daher werden mehrere Listen angelegt, die dann auch nicht immer alle griffbereit sind.

Besser ist daher ein Passwort-Buch, das ausreichend Platz für alle Ihre Passwörter bietet. Dazu reicht ein handelsübliches Notizbuch im Format DIN A6 mit rund 100 Seiten. Es gibt aber auch fertige Passwort-Bücher, die ähnlich wie Adressbücher aufgebaut sind und für jeden Eintrag folgende Zeilen enthalten:

- Name des Kontos/Geräts
- Webseite
- Anmeldename/Benutzername
- Passwort
- Sicherheitsfragen
- Bemerkungen

Ich verwende das Passwort-Buch „Password Keeper“ a, das Sie zum Preis von 6,99 € bei Amazon erhalten. Es hat mit 160 Seiten ausreichend Platz für meine vielen Passwörter und einen originellen Tresor-Aufdruck. Durch seine Griffmulden b haben Sie schnellen Zugriff auf den Inhalt und mit dem praktischen Gummiband c fixieren Sie beim Lesen oder Schreiben die Seiten.



Der Einband des Passwort-Buchs Password Keeper (links) und das aufgeschlagene Buch mit den Vordrucken für Ihre Passwort-Einträge (rechts).

Empfehlenswert ist auch das gut organisierte „Passwort-Buch“ von Ingmar Zastrow zum Preis von 5,89 €.

Meine Empfehlung: Bewahren Sie Ihr Passwort-Buch sicher auf, wenn Sie Ihren PC verlassen, damit es nicht gestohlen wird oder ein Unbefugter Ihre Passwörter heraussucht.

Methode 7: Überprüfen Sie Ihre neuen Passwörter: Sind sie wirklich sicher?

Haben Sie mit den Methoden 2 bis 4 Ihre neuen Passwörter gefunden, bleibt eine bange Frage: „Sind diese Passwörter wirklich sicher?“ Die Antwort liefert Ihnen ein vertrauenswürdiger Passwort-Prüfdienst. Verwenden Sie nur einen Dienst, der eine sichere, verschlüsselte Verbindung aufbaut. Der Dienst darf Ihre Passwörter nicht speichern und sollte von einem vertrauenswürdigen, deutschen Anbieter stammen. Ich empfehle Ihnen Checkdeinpasswort des deutschen Sicherheitsdienstleisters Mecodia GmbH. Das Angebot wird durch das Land Baden-Württemberg gefördert.

Für das Überprüfen Ihrer Passwörter benötigen Sie mit dieser Schritt-für-Schritt-Anleitung keinerlei Vorkenntnisse:

1. Rufen Sie zuerst die Testseite **checkdeinpasswort.de** auf.
2. Geben Sie ins Eingabefeld das Passwort ein, das Sie auf Sicherheit überprüfen möchten. Anstelle des eingegebenen Passworts werden zur Sicherheit Punkte angezeigt, damit das Passwort nicht von Umstehenden ausgespäht werden kann. Klicken Sie im Sicherheitssiegel auf das Wort **HIER**, erhalten Sie Informationen zu den Datenschutzgrundsätzen des Anbieters.
3. Während Ihrer Eingabe erfolgt bereits eine Bewertung. Sie sehen, wie sich die Sicherheit mit der Länge des Passworts und je nach Zeicheneingabe verändert. Geben Sie zum Beispiel **123456** ein, also eines der am einfachsten zu knackenden Passwörter, lesen Sie darunter, dass das einfache Passwort **123456** sofort geknackt werden kann.
4. Überprüfen Sie Ihre Passwörter nun nacheinander.
5. Lesen Sie immer alle Bewertungen, insbesondere die in gelber und roter Farbe. Sie geben Ihnen Anregungen, was beim betreffenden Passwort verbessert werden kann.

Meine Empfehlung: Ändern Sie Passwörter, bei denen der Hintergrund des Dienstes rot wird, sofort. Wie Sie an der wechselnden Farbe erkennen, wird Ihr Passwort mit jedem weiteren Zeichen etwas sicherer.

Meine Sicherheitsgarantie: Tappen Sie nicht in die Bequemlichkeits-Falle, bei der Sie einfachste Standard-Kennwörter einsetzen. Erstellen Sie Ihre Passwörter über meine 7 Sicherheitsmethoden. Nur so können Sie sich in Sicherheit wiegen, dass kein Hacker Ihre wichtigen Passwörter von Online-Konten oder Online-Diensten ergattert und Ihnen Böses will. Jetzt schützen Sie Ihre Daten sicher und beispielhaft!