Ein sicheres Passwort ist im Digitalzeitalter unerlässlich!

Das Wichtigste zu sicheren Passwörtern in Kürze

- Ein sicheres Passwort sollte **mindestens acht Zeichen lang** sein (besser mehr) und **sowohl Buchstaben, Zahlen als auch Sonderzeichen** enthalten.

- Vermeiden Sie Wortkombinationen oder logische Zahlen- oder Buchstabenreihen. Formen Sie stattdessen etwa Passwörter, die auf einem persönlichen **Merksatz** oder komplett **unreflektierte Zeichenreihen** beruhen.

- Nutzen Sie **für jede Registrierung ein neues, sicheres Passwort**. Sollte eines doch einmal geknackt werden (denn kein Passwort ist 100-prozentig sicher!), bleiben andere Zugänge dennoch geschützt.

- **Ein sicheres Passwort ist nur die halbe Miete**: Virenschutz, Firewall und ein sorgsamer Umgang mit den Logindaten sind ebenfalls unerlässlich, um den Schutz vor Datendiebstahl maximal zu optimieren.

Inhalt

Sichere Passwörter schützen sensible Daten und die Privatsphäre

PC, Laptop, Smartphone: Wir befinden uns mitten im digitalen Zeitalter und die meisten Menschen sind immer und überall vernetzt. Gerade das **World Wide Web aber birgt zahlreiche Gefahren** für die Privatsphäre eines jeden. Zahlreiche Schadsoftware zieht täglich ihre Bahnen durch das Internet und erreicht nicht nur über das elektronische Postfach die teils arglosen User. Um **sensible Daten** wie Bankverbindungen, aber auch andere personenbezogene Daten und private Bilderschätze gegen potentielle Angriffe besser abzuschützen, **kommt der Passwort-Sicherheit ein immer höherer Stellenwert zu**. Doch auch bei der Wahl eines Passwortes sind viele noch immer zu nachlässig. Auch weiterhin lassen die beliebtesten Eingaben die nötige Passwortstärke vermissen.

Nach einer **Erhebung des Hasso-Platter-Instituts für Softwaresystemtechnik (HPI)** zeigt sich, dass auch **2016** noch die beliebtesten Passwörter alles andere als sicher sind. Im Folgenden die **Top 10 in Deutschland**:

1. ***hallo***
2. ***passwort***
3. ***hallo123***
4. ***schalke04***
5. ***passwort1***
6. ***qwertz***
7. ***arschloch***
8. ***schatz***
9. ***hallo1***
10. ***ficken***

Kreativität Fehlanzeige und noch schlimmer: **Keines dieser Beispiele ist ein Anwärter auf den Titel "sicheres Passwort"**. Das zeigt sich schon in der Tatsache, dass die Beliebtheit dieser Passwörter extern abgelesen werden kann. Um Hackern nicht Tür und Tor zu öffnen, sollten Sie grundsätzlich von allzu leichten Passwörtern Abstand nehmen.

“Wie sicher ist mein Passwort?” – Der erste Schritt in die richtige Richtung

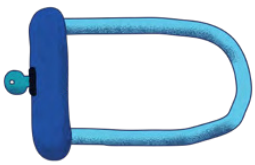
Finden Sie sich in der obigen Liste wieder oder sind die von Ihnen gewählten Passwörter in Sachen Sicherheit ähnlich angreifbar? **Testen Sie sich selbst und hinterfragen Sie Ihre Vergabepraxis**. Wenn Sie wissen wollen, ob Sie gute Passwörter gewählt haben, sollten Sie die nachfolgende **Liste mit hilfreichen Tipps** einer genaueren Betrachtung unterziehen:

7 Tricks für ein sicheres Passwort

1. **Vermeiden Sie Wiederholungen oder Tastaturmuster**. Von qwertz bis 1234321 sollten Sie folglich immer Abstand nehmen, wenn Sie auf der Suche nach einem guten Passwort sind.

2. Sie sollten zudem **keine Wörter nutzen**, die sich so auch in jedem Wörterbuch einfach nachschlagen ließen. Hier können Sie ggf. einzelne Buchstaben gegen **ähnliche Sonderzeichen** austauschen (Bsp. Passwort > Pa§$w0rt). Entsprechende Ähnlichkeiten lassen sich aber auch von geübten Personen allzu schnell durchschauen. **Namen und Geburtsdaten**, die sich allzu leicht auf Sie oder Ihr Umfeld beziehen lassen, sollten absolut Tabu sein.

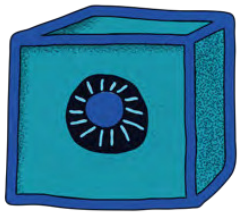
3. Vergessen Sie bei der Erstellung von Passwörtern nicht die Shift-Taste auf Ihrer Tastatur. Ein sicheres Passwort sollte **sowohl Groß- als auch Kleinbuchstaben** enthalten.



4. **Umlaute sollten Sie hingegen vermeiden**. Sollten Sie einmal einen PC im Ausland nutzen wollen, kann dessen Tastatur diese ggf. vermissen lassen, wodurch die Passworteingabe erheblich erschwert wäre.

5. Variieren Sie: Neben Buchstaben sollten **auch immer Zahlen und insbesondere Sonderzeichen** wie /[(%&§$_:?!+#)]\ aufgenommen werden. Nicht immer kann aus dem gesamten Pool der Sonderzeichen ausgewählt werden. Es sollten aber stets ein paar enthalten sein – und zwar nicht einfach als Anhängsel für ein Wort oder eine Zahlenreihe. Ihr Motto sollte lauten: **“Mittendrin, statt nur dabei!”**

6. Wenn Sie ein sicheres Passwort erstellen wollen, ist nicht nur der Ausdruck selbst, sondern auch dessen **Länge** von Bedeutung. Wollen Sie Dateien oder Zugänge mit einem guten Passwort verschlüsseln, sollte dieses **mindestens acht Zeichen** lang sein. Bei wichtigen Verschlüsselungen wie etwa dem **WLAN-Passwort** sollten Sie gute Passwörter von **mindestens 20 Zeichen** aus Zahlen, Buchstaben und Sonderzeichen wählen.



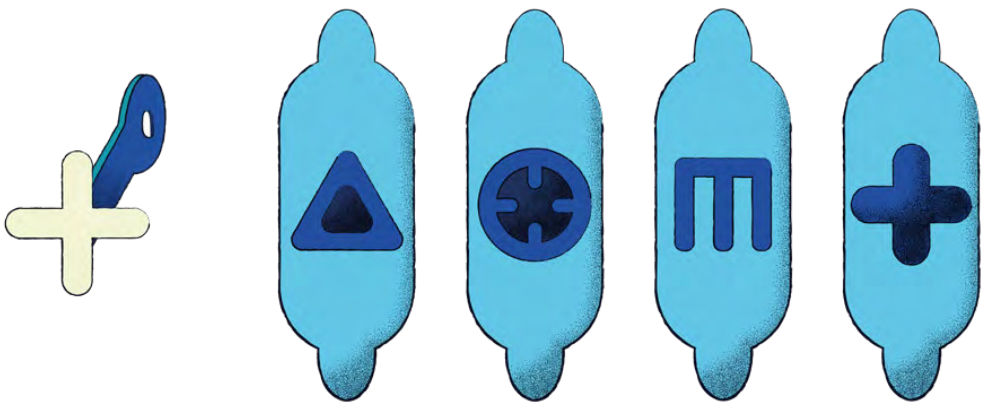
7. Sie können darüber hinaus auch **Sätze als Grundlage** nehmen, wenn Sie ein sicheres Passwort erstellen wollen. Denken Sie sich einfach einen für Sie einprägsamen Satz aus. Nun können Sie die Anfangsbuchstaben jedes Wortes zusammensetzen und ggf. auch einzelne Bestandteile durch Sonderzeichen ersetzen (Bsp. Mein Auto steht seit Januar 2017 in der Garage. > MAs$01/17@dG). Ein derart **kryptisches Passwort** lässt sich von Dritten nicht ohne Weiteres nachvollziehen.

Wichtig: Ein sicheres Passwort ist auch nur solange sicher, wie kein anderer es in die Hände bekommt. Sie sollten deshalb grundsätzlich sämtliche Passwörter **auswendig** kennen. Wollen Sie eine **schriftliche Absicherung** haben – etwa auch für Verwandte und Angehörige so Ihren digitalen Nachlass zugänglich machen – sollten Sie die Aufzeichnungen **sicher aufbewahren** und keinesfalls auf dem PC oder anderen elektronischen Geräten frei zugänglich ablegen.

Passwort-Sicherheitscheck online: Empfehlenswert oder nicht?

Wollen Sie bei Ihrem gewählten Passwort die Sicherheit prüfen, sollten Sie insbesondere **bei Online-Angeboten Vorsicht walten lassen**. Es ist grundsätzlich nicht empfehlenswert, ein Passwort auf zahlreichen Websites einzugeben. Die Daten können so leicht von Dritten und den Seitenbetreibern eingesehen und gesammelt werden.

Im Zweifel könnte sich durch Ihre IP-Adresse und andere übermittelte Informationen der Weg zu unterschiedlichen Accounts zurückverfolgen lassen. In eines dieser Schlösser könnte der Schlüssel schließlich passen.



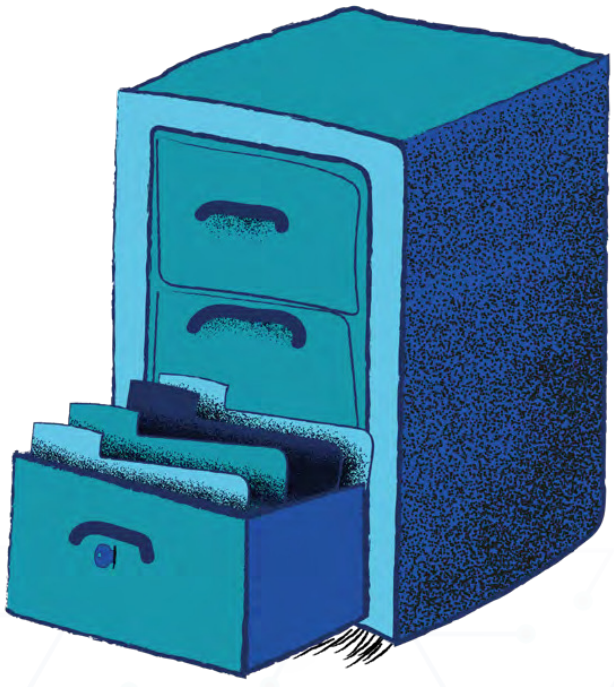
Wollen Sie ein sicheres Passwort, **testen Sie es lieber analog und prüfen Sie, ob Sie die Grundvoraussetzungen bei der Erstellung beachtet haben**: Länge, Zeichenvielfalt, Kryptologie usf. So können Sie im Internet für besseren Datenschutz sorgen. Sie können sich bei der Erstellung entsprechender Vorschläge von unterschiedlichsten Programmen unterstützen lassen.t

Alternative fürs Speichern: Kennwort-Tresor

Sie können alternativ auch auf unterschiedliche **Tresor-Programme** zurückgreifen, um Ihre Passwörter sicher zu speichern. Anwendungen von **Kaspersky** und Programme wie **LastPass oder True Key** können zum Teil auch als Browser-Plugin die Zugänge zu sämtlichen Online-Konten recht gut absichern und leicht zugänglich machen.

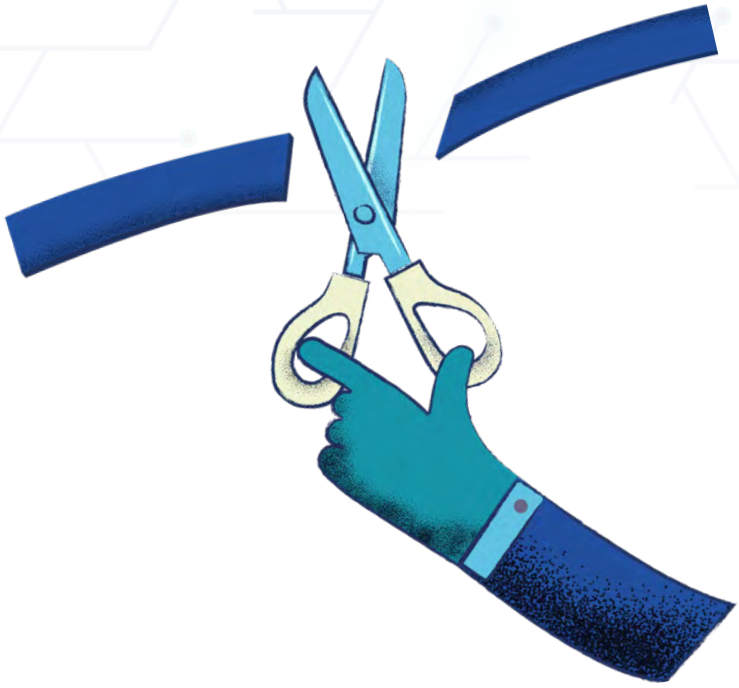
Mit deren Hilfe können Sie in der Regel nicht nur **für jeden Login ein sicheres Kennwort generieren**, sondern diese auch vergleichsweise sicher speichern. In der Regel benötigen Sie dann nur noch ein **Masterpasswort**, dass den Zugang zu dem Tresor schützt. Je mehr Kennwörter Sie in den Programmen hinterlegen, desto sicherer sollte mithin auch Ihr Masterpasswort sein.

Wichtig: Sie sollten grundsätzlich für jeden neuen Zugang auch ein neues, sicheres Passwort verwenden. So verringern Sie die Gefahr, dass, sollte eines Ihrer Kennwörter doch einmal geknackt werden, noch zahllose andere Türen für die Datenpiraten offenstehen. Tresor-Software kann dann das Merken erleichtern. Aber auch diese ist nicht unangreifbar.



Ob im Leben oder im WWW: Es gibt keine 100-prozentige Sicherheit!

Ein absolut unknackbares Passwort gibt es nicht – ebensowenig wie ein unknackbares Schloss im Real Life. Ein sicheres Passwort soll vielmehr den Zugang erheblich erschweren, denn: Je mehr Zeit für den digitalen Einbruch aufgewendet werden muss, desto größer ist die Wahrscheinlichkeit, dass Datendiebe von dem Vorhaben abweichen.



Es zeigt sich nicht selten, dass vor allem Zugänge und Daten von Personen geklaut oder missbraucht werden, **die es den Dieben allzu leicht machen**. Geringer Aufwand bedeutet dann nämlich oft auch schnelleren Profit bzw. Erfolg. Im Allgemeinen gilt dabei: Je komplexer das gewählte Passwort, desto länger benötigen Hacker für deren Entschlüsselung oftmals (Glückstreffer ausgeklammert).

Ein sicheres Passwort soll also vor allem: Zeit schinden. Verbunden mit der generellen Empfehlung, die **Passwörter regelmäßig zu wechseln** und neu zu vergeben, wird der Zugang zu persönlichen und empfindlichen Daten so erheblich erschwert. Wenn auch keine 100-prozentige Sicherheit zu erreichen ist, so lässt sich über die Länge und Gestaltung des Passwortes doch das **Sicherheitslevel maßgeblich erhöhen**.

Brute Force, Malware & Co.: Wie wird selbst ein sicheres Passwort geknackt?

Den Datendieben stehen zahlreiche Möglichkeiten zur Verfügung, um an sensible und kostbare Informationen zu gelangen – ob nun für den Datenhandel oder den Zugriff auf Konten.

Angriffsziel sind dabei jedoch zunächst nicht die reinen Passwörter, **sondern die als Hash hinterlegten Übersetzungen** dieser. Das **englische Verb *to hash*** bedeutet so viel wie "**zerhacken, zerkleinern**". Legen Sie bei der Registrierung bei einem Online-Dienst wie z. B. Facebook ein Passwort fest, wird dieses nicht als Klartext auf dem Server gespeichert, sondern in **einen Hash-Algorithmus zerlegt** bzw. übersetzt (komplexe Reihen aus Kleinbuchstaben und Zahlen). Die Übertragung folgt komplexen mathematischen Formeln und Berechnungen.

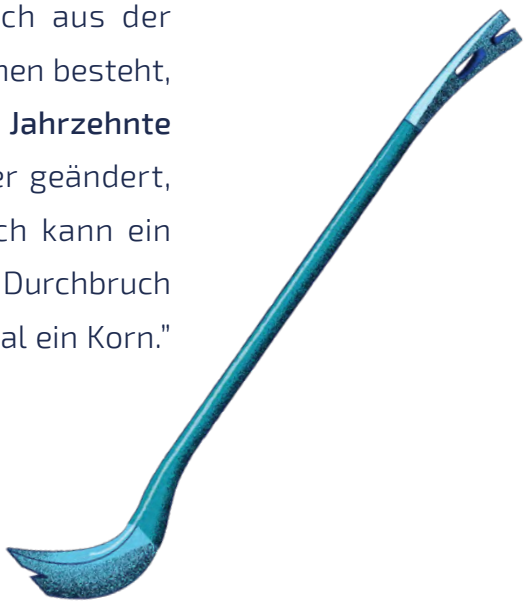
Wollen Sie sich nach der erfolgreichen Registrierung mit Ihren Zugangsdaten einloggen, wird das erneut eingegebene sichere Passwort wieder zerlegt. Der **aktuelle Hash** wird mit dem bei Registrierung auf dem Server **hinterlegten Hash verglichen**. Stimmen beide Informationen überein, lässt der Server Sie auf die Website und Ihr Profil zugreifen.

Bei großangelegten Attacken auf Server sind gerade **diese Hashs das eigentliche Angriffsziel**, da sich aus diesen die Passwörter wieder zusammensetzen lassen können. Dabei sind unterschiedliche Methoden möglich:

Brute Force

Eine sogenannte **Attacke der rohen Gewalt** (Brute-Force-Attack) ist eher die grobschlächtige Variante: Der Datendieb versucht gewissermaßen, mit dem **Brecheisen** das Schloss zu öffnen. Über unterschiedliche Einstellungen kann ein Hacker einen Computer anweisen, unzählige Zeichenfolgen zu erstellen (mehrere Millionen pro Sekunde). Die **sich hieraus ergebenden Hashs kann er mit den bereits erbeuteten Hashs vergleichen** und so Rückschlüsse auf die entsprechenden Passwörter ziehen.

Ein sicheres Passwort, das nicht nur lang ist, sondern auch aus der beliebigen Kombination von Zahlen, Buchstaben und Sonderzeichen besteht, kann den Computer dabei **schon mal mehrere Jahre und sogar Jahrzehnte beschäftigen**. Wurde das Passwort in diesem Zeitraum wieder geändert, verzögert sich die Entschlüsselung noch zusätzlich. Natürlich kann ein **Glückstreffer** auch beim sichersten Passwort schon früher zum Durchbruch führen – ganz nach dem Motto: "Auch ein blindes Huhn findet mal ein Korn."

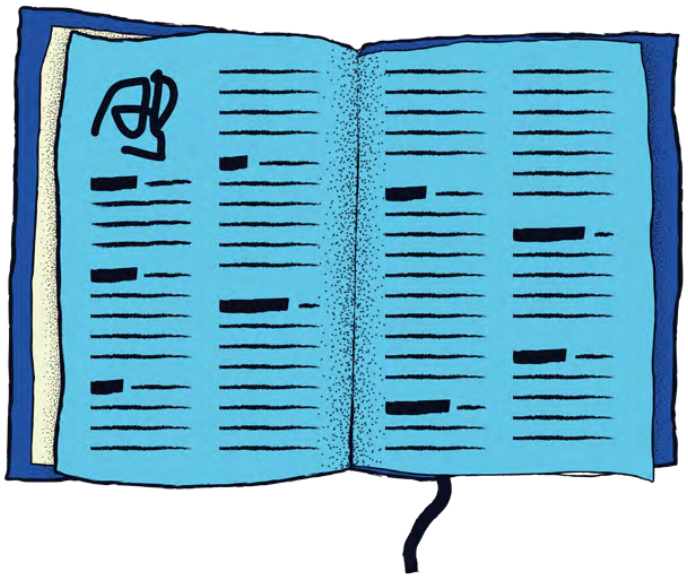


Hierin zeigt sich: **Ein sicheres Passwort macht es den Angreifern in der Regel sehr schwer, den Hash zu rekonstruieren.** Je länger und komplexer das Passwort, desto besser. Auch wenn das Abgreifen der Hashs von den Servern vom User selbst nicht verhindert werden kann, so kann er den Angreifern den Weg zum endgültigen Erfolg wesentlich erschweren.

Angriff der Wörterbücher

Eine **Dictionary-Attack** kann gegen ein sicheres Passwort in der Regel nichts aussetzen, sondern zielt vor allem auf diejenigen User ab, die sich bei der Wahl ihrer Kennwörter auf einfache Wörter stürzen, **die in Wörterbuch, Lexikon & Co. leicht zu finden sind**. Angreifer können diese als Basis für die Aufschlüsselung nehmen, da noch immer zu viele Menschen einfache Wörter, Markennamen oder Namen von Stars als Passwörter nutzen.

Beim Durchspielen der Wörter lassen diese sich im Gegensatz zur Brute-Force-Attack **ungleich schneller aufschlüsseln**. Selbst die Kombinationen mit angefügten Zahlen (etwa Geburtsjahren) oder einfachen Satzzeichen können Hacker dabei bereits regelmäßig einbeziehen.



Abgreifen des Passwortes direkt beim User

Neben diesen komplexen Abläufen können Datendiebe aber auch auf wesentlich **einfachere und schnellere Varianten** zurückgreifen, um an die Passwörter von Usern zu gelangen. Die meisten nutzen dabei die **Leichtgläubigkeit** der Internetnutzer aus. Hier wird ein Passwort auf direktem Weg vom Verbraucher selbst abgefragt – auf mal mehr, mal minder gerissene Art (z. B. über Phishing-Mails, in sozialen Netzwerken verbreitete Links zu Seiten, wo das Passwort eingegeben werden soll usf.). Der Datenschutz spielt also auch bei E-Mails eine große Rolle.

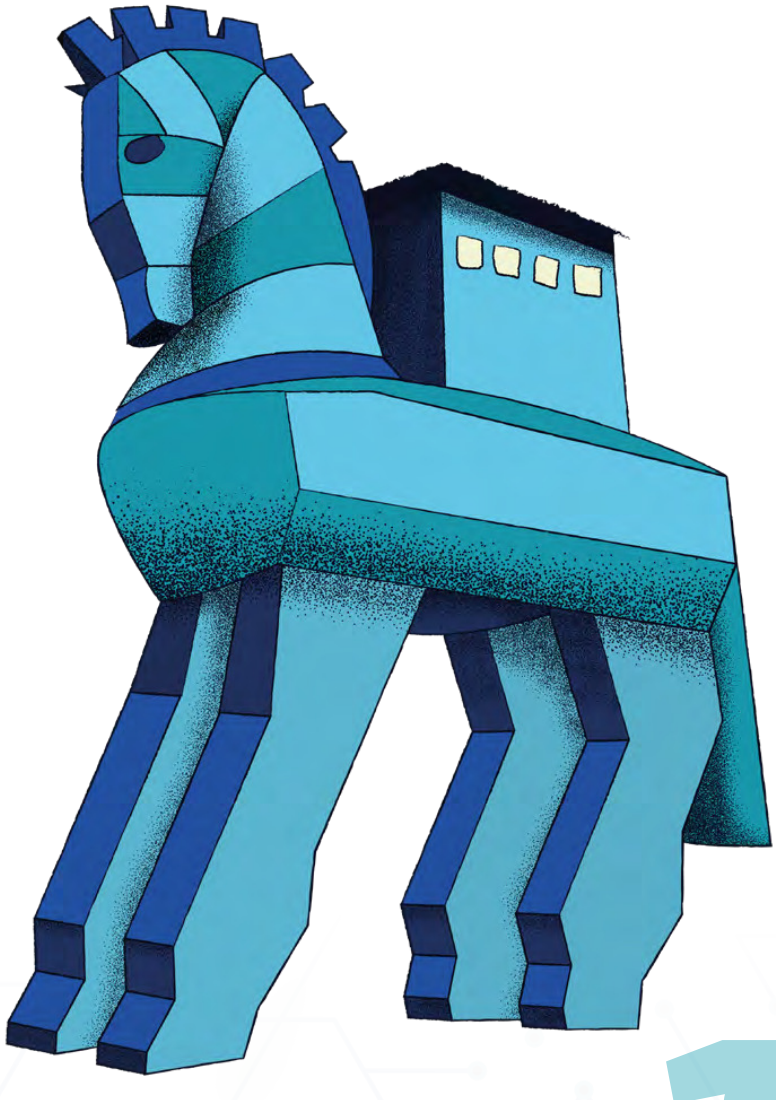
Im Übrigen: **Sie sollten auch immer sichergehen, dass niemand einen Blick auf Ihre Tastatur oder Ihr Passwort erhaschen kann, wenn Sie dieses eingeben.** Das ist nämlich noch immer die leichteste Art, Kennwörter abzugreifen. Während die meisten Menschen bei der Bargeldabhebung diesbezüglich immer stärker sensibilisiert sind, fehlt diese Vorsicht nicht selten bei der Eingabe von Passwörtern an PC, Tablet & Co. Ob unter Kollegen, Freunden oder innerhalb der Familie: Vertrauen ist gut, Kontrolle ist besser, um dem Datenmissbrauch vorzugreifen!

Und auch **Schadprogramme**, die oftmals im Gepäck nicht vertrauenswürdiger Downloads auf PC und Smartphone landen, können zum Teil recht unkompliziert etwa die Tastatureingaben abgreifen oder Informationen auf dem Computer auslesen und weiterleiten. Deshalb ist ein sicheres Passwort stets nur die halbe Miete. Auch **Schutzsoftware** sowie eigenes Verhalten bestimmen, wie gut ein Kennwort am Ende tatsächlich ist.

Nicht nur ein sicheres Passwort für angemessenen Schutz erforderlich!

Um den Schutz der eigenen automatisierten Daten noch weiter zu erhöhen, sollten auf allen elektronischen Endgeräten zusätzlich auch immer weitere Programme installiert sein – vergessen Sie dabei Ihr Smartphone nicht. Wichtig sind dabei vor allem **Antivirenprogramme und Firewalls**, die das Eindringen von Schadsoftware verhindern.

Damit die Tür für T**rojaner, Viren, Würmer, Spyware & Co.** versperrt bleibt, sollten die Schutzprogramme in jedem Fall stets auf dem aktuellsten Stand sein. Führen Sie also **regelmäßig Updates** durch.



Impressum

Unter diesem Link gelangen Sie zu unserem Impressum: Impressum