
# Die fünf häufigsten Passwort-Fehler

Ein schlechtes Kennwort lädt Kriminelle förmlich ein, Sie zu bestehlen. Damit Ihnen das nicht passiert, sollten Sie die fünf schlimmsten Passwort-Fehler kennen. Außerdem finden Sie Tipps für ein perfektes Kennwort.

Von **Arne Arnold** und **Benjamin Schischka**

**Beim Online-Banking,** fürs Mailpostfach, bei Amazon und vielen weiteren Diensten brauchen Sie ein Kennwort. Das nervt und kann dazu verleiten, ein Standardpasswort zu benutzen. Genau das machen viele Anwender – und haben damit schon einen der häufigsten Passwort-Fehler begangen. Diese Fehler kennen und nutzen natürlich auch die Cyber-Kriminellen aus.

Damit Sie davor gefeit sind, haben wir die fünf schlimmsten Fehler rund um Passwörter zusammengestellt. Außerdem finden Sie Tipps, wie Sie sichere Kennwörter erstellen und mit einem Gratis-Tool auf CD/DVD perfekt verwalten.

## Fehler 1: Das Passwort ist zu kurz – es lässt sich leicht knacken

Oft wählen Anwender kurze Passwörter, weil sie leichter zu merken sind. Dieses Plus an Bequemlichkeit geht aber deutlich zu Lasten der Sicherheit. Ein Rechenbeispiel zeigt, wie lange ein Passwort einer Brute-Force-Attacke standhalten kann. So bezeichnet man den Vorgang, wenn eine Software alle möglichen Zeichenkombinationen ausprobiert. Angenommen, ein Passwort ist sechs Zeichen lang und besteht nur aus Kleinbuchstaben. Dann kommen 26 verschiedene Zeichen in Frage, was insgesamt 308.915.776 Kombinationen zulässt. Das hört sich zunächst nach viel an. Doch ein PC mit einer schnellen CPU und einem entsprechend optimierten Tool knackt es in nur 10 Sekunden!

**Tipp:** Ein sicheres Passwort ist mindestens acht Zeichen lang und enthält Groß- und Kleinbuchstaben. Per Brute Force sind dann schon zwei Monate nötig. Sonderzeichen und jede weitere Stelle verlängern die Berechnung um ein Vielfaches. Wer das Kennwort auch im Ausland benutzen will, verzichtet besser auf Sonderzeichen. Oder Sie informieren sich vorab, über welche Tastenkombinationen sie auf ausländischen Tastaturen zu erreichen sind.

## Fehler 2: Das Passwort ist zu einfach – es lässt sich erraten

Ein Kennwort ist genau dann zu einfach, wenn es nur aus einem Wort besteht und es sich in einem Wörterbuch finden lässt. Die Länge spielt dabei eine geringere Rolle. Denn die einfachste Knackmethode ist die Wörterbuch-Attacke. Dabei probiert ein Knack-Tool der Reihe nach alle Wörter aus, die in einem solchen Buch stehen. Selbst Standard-PCs benötigen für den kompletten Durchlauf mit einem Wörterbuch mittleren Umfangs nicht allzu lange.

In solch ein Wörterbuch lassen sich auch Zahlenlisten aufnehmen. Deshalb sind als Kennwort auch Geburtsdaten nicht empfehlenswert. Ebenfalls zu einfach sind Passwörter, die einem bestimmten Muster folgen. Vermeiden Sie also Zeichenfolgen wie „12345“ oder „qwertz“, aber auch „abcdef“.

**Ein Beispiel:** Mit „happiness“ hatte ein Mitarbeiter vom englischsprachigen Dienst Twitter (*www.twitter.com*) versucht, sein Profil zu schützen. Ein 18jähriger Hacker hatte über Nacht eine Wörterbuch-Attacke gegen dieses Profil laufen lassen und fand am nächsten Tag das richtige Passwort vor. Da es das Profil eines Admins war, hätte er anschließend jeden anderen Account in Beschlag nehmen können. Möglich war die Attacke, da Twitter belie-

big viele Versuche beim Einloggen zuließ. Das ist übrigens auch bei vielen anderen Online-Diensten der Fall.

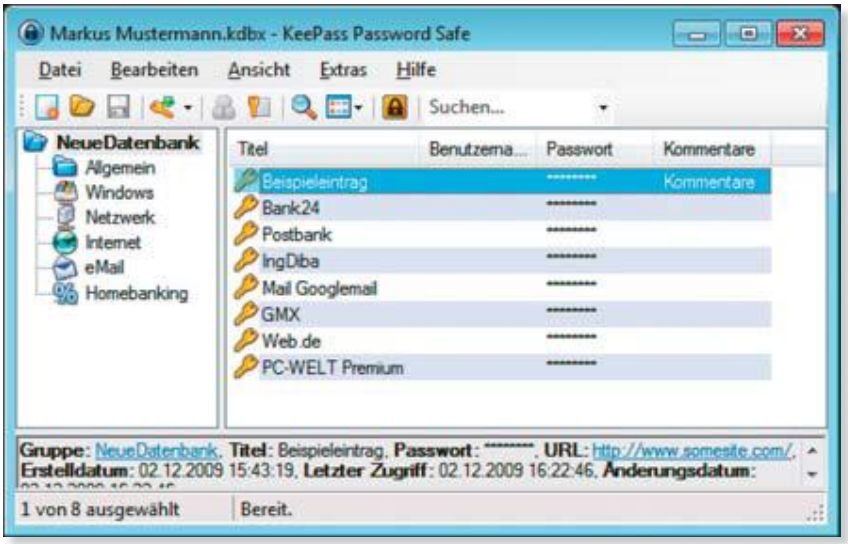
**Tipp:** Ein gutes Passwort sollte nicht in einem Wörterbuch vorkommen, also sinnfrei sein.

## Fehler 3: Aufschreiben und Speichern von Passwörtern

Selbst das sicherste Passwort kann schnell wertlos sein, wenn es unverschlüsselt auf der Festplatte gespeichert wird. Denn Schad-Software und Hacker können es dann stehlen. Mancher Anwender sendet seine Passwörter auch an sein eigenes Mailpostfach, um es von überall aus abrufen zu können. Oder er notiert es auf einem Blatt Papier, wo es von anderen gelesen werden kann.

**Tipp:** Am besten ist es, sich sämtliche Passwörter zu merken. Bei wirklich komplizierten Kennwörtern ist das aber schwer. Will man sie speichern, empfiehlt sich ein Passwort-Safe, in dem die Codes verschlüsselt gelagert werden. Der Safe selbst ist dann mit einem Master-Passwort versehen. Es sollte sehr sicher sein, da es die einzige Hürde vor sämtlichen Kennwörtern darstellt. Außerdem sollten Sie es auf keinen Fall notieren. Ebenso fatal wäre es, dieses Master-Passwort zu vergessen, da Sie dann den Zugriff auf alle Codes verlieren. Knacken lässt sich das gute Passwort ja nicht.

Um Ihre Kennwörter sicher zu speichern, können Sie das kostenlose Programm **Keepass Password Safe 2.09** nutzen. Sie finden es auf ◉ CD/DVD und unter *http://keepass.info*. Es läuft unter XP, Vista und Windows 7. Für das Tool gibt's eine deutsche Sprachdatei (auf ◉ CD/DVD), die Sie ins Programmverzeichnis von Keepass speichern. Über „View, Change Language" stellen Sie auf die deutschsprachige Benutzerführung um.




**Passwort-Safe:** Mit der Freeware Keepass speichern und verwalten Sie alle Passwörter sicher in einem verschlüsselten Container. Zu den Kennwörten lassen sich beliebige Informationen speichern

## Fehler 4: Seit Jahren dasselbe Passwort verwenden

Viele Anwender nutzen seit Jahren dasselbe Passwort. Das ist gefährlich. Denn unter Umständen merkt man gar nicht, dass das Passwort ausgespäht wurde. Ein Hacker hat im Idealfall also zeitlich unbegrenzten Zugang und kann so beispielsweise den Mailverkehr über Monate oder gar Jahre mitlesen.

**Tipp:** Ändern Sie Ihre Passwörter regelmäßig. Dafür ist jede Menge Kreativität gefragt. Besser ist es, einen Passwortgenerator einzusetzen. Keepass Password Safe (Infos siehe oben) bringt gleich einen solchen mit. Sobald Sie dort einen neuen Eintrag erstellen, liefert das Tool ein sicheres Passwort. Ein Klick auf das Icon neben dem Passwortfeld macht es sichtbar. Weitere Kennwörter gibt's per Knopfdruck.

Welche Bedingungen das Passwort erfüllen muss, legen Sie über „Extras, Passwort generieren" fest. Dort sollten Sie „Sonderzeichen" aktivieren.

## Fehler 5: Immer ein und dasselbe Passwort nutzen

Mailadressen, Windows, ZIP-Archive, Facebook, Foren, ICQ – schnell kommt ein ganzer Haufen an Passwörtern zusammen. Ein beliebter Fehler besteht darin, auf einen Zugangscode für alle Dienste zu setzen. Das ist zwar bequem, weil man sich nur eines merken muss. Doch hat jemand es erst einmal gestohlen oder geknackt, dann ist der Schaden riesig. Der Eindringling hat nämlich mit einem Schlag Zugriff auf alle Internet-Dienste, die Sie nutzen. Tatsächlich ist es unter Hackern üblich, geknackte Passwörter auch bei anderen Log-ins zu testen.

**Tipp:** Verwenden Sie für jeden neuen Log-in ein eigenes Passwort. Sperren Sie die diversen Zugangscodes in einen Tresor wie Keepass Password Safe.

## Fazit: So sieht ein gutes, fast unkackbares Passwort aus

Ein gutes Passwort ist möglichst lang – Minimum sind acht Zeichen. Es enthält Klein- und Großbuchstaben sowie Zahlen und Sonderzeichen. Achten Sie darauf, dass es nicht in einem Wörterbuch vorkommt. Idealerweise lassen Sie sich Kennwörter von einem Generator erzeugen, wie ihn Keepass Password Safe bietet. Speichern Sie Ihre Zugangscodes niemals unverschlüsselt auf Ihrem PC. Notieren Sie sie nicht auf einem Zettel, den andere einsehen könnten. Wechseln Sie jedes Passwort alle paar Wochen.

## FINGER WEG VON DIESEN PASSWÖRTERN

**Das Sicherheitsunternehmen McAfee** (*www.mcafee.de*) hat die gebräuchlichsten Passwörter in Europa ermittelt. Bei jedem Kennwort wird mindestens ein gravierender Fehler gemacht. An der Umfrage nahmen rund 3500 Anwender teil.

1. Name eines Haustiers
2. Ein Hobby
3. Mädchenname der Mutter
4. Geburtsdatum eines Familienmitglieds
5. Eigenes Geburtsdatum
6. Name des Partners
7. Eigener Name
8. Lieblingsfußballmannschaft
9. Lieblingsfarbe
10. Name der ersten Schule