# HowTo Gute Kennworte


2020-06-08

# Contents

# 1 Was muss ich wissen?

Dieses HowTo soll einen einfachen Überblick über das Thema „sichere Passwörter“ schaffen.

Aufgrund der Komplexität von Passwörtern und deren Einsatz kann dieses HowTo auf keinen Fall als abschließend oder als vollständig betrachtet werden, sondern soll einzig als Hilfestellung und Richtlinie dienen.

Dieser Umstand ist immer zu berücksichtigen und es empfiehlt sich daher in diesem Zusammenhang immer mit besonderer Sorgfalt und Bedacht zu agieren.

Passwörter dienen dem Schutz von IT-Geräten und Daten. Sie verhindern unbefugte Zugriffe. Deswegen sind die richtige Auswahl und der richtige Umgang enorm wichtig!

Besonders IT-Sicherheit als auch der Datenschutz unterliegen ständigen und laufenden Veränderungen. Schon morgen kann eine heute ausgesprochene Empfehlung nicht mehr gültig - weil überholt - sein.

# 2 Passwörter und technische Sicherheit

Die Auswahl eines guten Passworts ist entscheidend für die Sicherheit und Vertraulichkeit von Daten.

Gute Passwörter sind ausreichend lang (absolutes Minimum 10 Zeichen) und bestehen aus verschiedenen Arten von Zeichen wie Groß- und Kleinbuchstaben, Zahlen, Sonder- und Satzzeichen, die zusammen kein sinnvolles Wort ergeben sollten.

Alternativ können ausreichend lange und individuell abgewandelte Passphrasen verwendet werden.

Im Allgemeinen ist das Anmeldepasswort der erste und entscheidende Schutz eines Computers vor Datendiebstahl und Manipulationen jeglicher Art.

Für die Anmeldung an Internet-Diensten wie bspw. Webmail, Facebook, ebay, PayPal, OnlineBanking sollte niemals nur ein einziges Passwort verwenden. Wird eine dieser Websites „gehackt“, hätte der Angreifer Zugriff auf alle verwendeten Webdienste.

# 3 Der richtige Umgang

Passwörter - insbesondere das Passwort für das Anmelden am Computer - darf nie weitergegeben werden. Auch nicht an Kolleginnen und Kollegen oder Vorgesetzte. Sollte die Weitergabe unbedingt notwendig sein, ist das Passwort anschließend sofort zu ändern.

Für verschiedene Anmeldungen sind verschiedene Passwörter einzusetzen. Durch kleine Variationen – z.B. durch die Änderung von drei Buchstaben des Passworts – ist dies leicht durchführbar und bleibt dennoch einfach zu merken.

Auf keinen Fall darf das gleiche Passwort für die Anmeldung am Computer und Anmeldungen im Internet (z.B. Webmail) verwendet werden.

# 4 Die richtige Auswahl

Hier kann nur eine grobe Übersicht für sichere Passwörter gegeben werden.

- Mindestens 10 Zeichen.
- Zufällige Zeichen aus verschiedenen Arten von Zeichen (Großbuchstaben, Kleinbuchstaben, Ziffern, Satzzeichen und Sonderzeichen). Nur Groß- und Kleinbuchstaben zu verwenden ist unsicher!
- Niemals Namen, Vornamen, Geburtsdaten, KFZ-Kennzeichen und ähnliche persönliche Daten verwenden! Diese werden bei Angriffen als erstes ausprobiert.
- Keine Begriffe aus einem Wörterbuch verwenden (auch nicht in einer anderen Sprache). Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
- Das Passwort ist nur mir selbst bekannt.
- Das Passwort wird nur für einen einzigen Dienst verwendet.
- Idealerweise ist das Passwort leicht zu merken; alternativ kann ein Passwortmanager verwendet werden, welcher komplexere Passwörter ermöglicht.
- Trivial Passwörter (qwertz, 4711 etc.) sind absolut ungeeignet. Diese können von Anderen leicht durch Beobachten der Passworteingabe erkannt werden.

# 5 Wie wird ein sicheres Passwort erstellt?

## 5.1 Die kurze Version:

Verwende einen Passwort-Generator!

## 5.2 Die ausführliche Version:

Gute Passwörter stehen und fallen mit der Zufälligkeit mit der sie erzeugt werden. Erwiesenermaßen sind Menschen immer äußeren Einflüssen ausgesetzt und daher nicht in der Lage wirklich zufällig zu agieren. Diese äußeren Einflüsse wirken oft unbewusst auf Menschen, und deshalb sind durch Menschen erzeugte zufällige Passwörter alles andere als zufällig. Diese sind in der Regel sehr einfach zu erraten oder abzuleiten.

### 5.2.1 Länge des Passworts

Über die Länge von sicheren oder starken Passwörtern lässt sich trefflich streiten.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt generell eine Mindestlänge von 8 Zeichen.

Eine Mindestlänge von 10 bis 12 Zeichen wird von IT-Experten eindringlich empfohlen.

Aus dieser Empfehlung ergeben sich aber durchaus auch Probleme, da viele Diensteanbieter die Zeichenzahl beschränken. Selbst aktuelle Online-Banking-Portale lassen für ein Login-Passwort oft nur 5(!) Zeichen zu.

Es herrscht die einhellige Meinung, dass mit Passwörtern von 15 oder mehr Zeichen Länge der durchschnittliche Benutzer ausreichend sicher sein sollte. Aus je mehr Zeichen und Arten von Zeichen ein Passwort besteht, desto mehr Kombinationsmöglichkeiten ergeben sich theoretisch.

### 5.2.2 Zeichen des Passworts

Ein sicheres Passwort ist so zufällig als möglich.

Es ist erwiesen, dass Menschen sehr schlecht darin sind etwas zufällig auszuwählen.

Ein Passwort sollte aus einem Zeichenvorrat mit möglichst vielen unterschiedlichen Zeichen erzeugt werden. Also aus Zeichen wie Groß- und Kleinbuchstaben, Zahlen, Sonder- und Satzzeichen. In Kombination mit der Länge des Passwortes bildet der Zeichenvorrat die wichtigsten Faktoren der Passwortsicherheit.

Das Passwort darf in keinem Wörterbuch - auch nicht Fremdsprachigen - vorkommen, und darf keine persönlichen Informationen wie Namen, Beruf, Geburtsdaten, Autokennzeichen und -marken oder Telefonnummern enthalten. Derartige Daten können leicht ermittelt werden und werden immer als Erstes ausprobiert.

Auch Trivialpasswörter, wie Buchstabenfolgen auf der Tastatur (qwertz) sind eine äußerst schlechte Wahl. Diese können mit hoher Wahrscheinlichkeit ermittelt werden.

### 5.2.3 Geheimes Passwort

Niemand ausser einem selbst darf ein Passwort kennen!

Man kann einen Passwort-Manager/Passwort-Safe einsetzen, um sich nicht jedes einzelne Passwort merken zu müssen.

### 5.2.4 Einzigartiges Passwort

Für unterschiedliche Anwendungen sind auch unterschiedliche Passwörter zu verwenden. Niemals das selbe Passwort für verschiedene Anwendungen verwenden!

Das sicherste Passwort bringt nichts wenn es für verschiedene Dienste oder Anwendungen genutzt, und einer der Dienste gehackt wird. Ein Hacker würde sofort versuchen, sich mit diesen Zugangsdaten auch bei anderen bekannten Diensten anzumelden.

### 5.2.5 Leicht zu merkendes Passwort

Ein Passwort ist idealerweise so aufgebaut, dass man es sich leicht merken kann.

Als Alternative gibt es die sogenannte Akronym-Methode. Bei dieser denkt man sich einen möglichst langen Satz aus, welcher auch individuellen und persönlichen Bezug hat. Er sollte daher möglichst einzigartig sein und muss auch keinen Sinn ergeben. Man bildet dann aus den Wortanfängen (oder einzelnen Buchstaben) das Passwort.

```
Beispiel:
    Ich kann mir nur ein Passwort leicht merken!
wird zum Passwort
    Ikmn1PWlm!
```

### 5.2.6 Passwort-Manager verwenden

Mit einem Passwort-Manager können mehrere, unterschiedliche Passwörter verwaltet und durch ein einziges Master-Passwort geschützt werden.

Dieses Master-Passwort muss sicher sein, also zumindest die vorstehend erwähnten Kriterien und Merkmale erfüllen.

Viele Passwortmanager unterstützen anstelle des Master-Passwortes auch die Option der Verwendung einer Schlüsseldatei oder eines Security-Token.

Diese Software speichert Passwörter verschlüsselt auf dem Computer. Nach Eingabe des Master-Passworts (zum Entsperren des Safes) sind alle gespeicherten Passwörter abrufbar. Manche Passwort-Manager generieren auch auf Knopfdruck sichere Passwörter.

Eine ganze Reihe derartiger Software ist kostenlos im Internet zu finden. Natürlich wäre OpenSource-Software zu bevorzugen.

Wenn der im Internet-Browser integrierte Passwort-Manager verwendet wird, sollte man auch hier die Option „Master-Passwort“ aktivieren.

Die Alternative dazu wäre - ganz analog - Papier und Stift. Die Gefahr, dass doch unbefugte Zugriff auf die Passwörter bekommt ist jedoch ungleich größer.

Besonders wichtige Passwörter sollte man am besten trotzdem im Gedächtnis haben, diese aber auch notieren und sicher - z.B. in einem Safe - verwahren.