

Wie man ein sicheres Passwort auswählt und behält

Meike Pfefferkorn - 2021-09-03 - Allgemeine Hinweise

Bei Passwörtern hat man die sprichwörtliche Qual der Wahl, sie sollten möglichst sicher sein und man möchte sie aber dennoch im Gedächtnis behalten können. Aber die sichersten Passwörter sind kryptisch und sehr lang und deshalb eher ungeeignet für ein menschliches Gedächtnis. Jedoch kann man sich auch einfach an ein paar Regeln halten um besonders einfach zu knackende Passwörter zu verhindern und dennoch ein sicheres auszuwählen. Passwortmanager wie z.B. KeePass helfen dabei viele Passwörter zu behalten und sicher abzuspeichern.

Passwortregeln

Zur Zeit sind die folgenden Sonderzeichen in einem Passwort erlaubt (inklusive Leerschlag):

: ; < > | = . , _ - ~ ! ? & % @ # \$ £ € ° ^ * § () + []

Und Minimum 8 Zeichen, besser aber verwenden Sie 12 oder bis zu 25 (s. Link unten), welche Klein- und Grossbuchstaben und Zahlen enthalten. Grundsätzlich gilt: Je länger desto besser.

[Link Sichere Passwörter](#)

[Link mit Anleitung für Passwortmanager](#)

[Link zur Übersicht aktueller Passwortmanagern](#)

[Link KeePass](#)

Wurde mein Login/eMail gehackt?

Es werden täglich Millionen von Logins gehackt und Daten gestohlen bzw. Passwörter benutzt um Schaden anzurichten wie z.B. Identitätsdiebstahl, illegale Käufe, Kartendetails downloaden usw. Sie können sich mit einem langen und nicht zu erratendem Passwort, für jeden Webservice ein anderes, gut dagegen schützen. Um zu überprüfen ob Ihre Logins jemals gehackt wurden können Sie diesen Service benutzen. Wurden Logins kompromittiert sollten Sie umgehend ein neues sicheres Passwort setzen!

[Wurde ich gehackt? Have I been pwned?](#)