

Sichere Passwörter – einfach erstellen

Niederösterreichischer Zivilschutzverband



**123456, querty, login,
password**

Passwörter werden heute überall gebraucht – am Handy, bei Apps, beim e-banken, am Arbeitsplatz. Bei der Flut an Passwörtern, die man den ganzen Tag immer wieder braucht, liegt es nahe, ein möglichst kurzes und einfaches Passwort zu wählen. Oder?

Schatzi, 1985, hallo123 – Die wichtigsten Infos zu sicheren Passwörtern

Passwörter nicht mehrfach verwenden!

Verwende für verschiedene Accounts/Apps/Dienste auch verschiedene Passwörter. Dadurch kann ein gehacktes Passwort nicht öfters verwendet werden.

Wie sieht ein möglichst sicheres Passwort aus?

Ein sicheres Passwort sollte möglichst lang und komplex sein. Also, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Um sich ein solches Passwort zu merken kann man Eselsbrücken verwenden – zum Beispiel die Anfangsbuchstaben eines Satzes den man sich leicht merkt. Buchstaben kann man dabei auch leicht gegen ähnlich aussehende Ziffern ersetzen, zum Beispiel I=1, E=3 usw.

Auf keinen Fall sollte man Wörter verwenden die im Wörterbuch stehen.

Wie soll ich mir das merken?

Wenn überhaupt, Passwörter nicht im Klartext aufschreiben. Den berühmten Zettel unter der Tastatur oder in der Schreibtischschublade sollte man mit Hilfe von Eselsbrücken oder Passwortmanagern verbannen. Empfehlenswert ist der Passwortmanager „Keepass“.

Aller guten Dinge sind Zwei!

Zwei-Faktor-Authentifizierung – nervig aber sicher. Durch die Zwei-Faktor-Authentifizierung erzeugt man eine zweite Barriere, so können Hacker selbst bei geknackten Passwörtern nicht auf den Account zugreifen. Dabei gibt man wie gewohnt die Anmelde-Daten ein (Name und Passwort) und tippt dann den, meist sechsstelligen, Pin ein – den man aufs Handy oder Tablet geschickt bekommt.

Zu bedenken ist hier allerdings das man das Smartphone dabei haben muss – sonst kommt man auch nicht hinein!

In aller Kürze, ein gutes Passwort ist:

- Lang
- Komplex
- Leicht zu merken (oder Passwortmanager verwenden)
- Nirgends notiert und nur ihnen bekannt
- Durch Zwei-Faktor-Authentifizierung geschützt

