

IN 8 SCHRITTEN ZUM STARKEN PASSWORT

Oder auch: Das müssen Ihre Angestellten wissen

01.

PASSWÖRTER WOLLEN EINZIGARTIG SEIN

Dies gilt für wirklich **jeden** Account. Sie wollen doch nicht, dass Kriminelle mit nur einem Hack mehrere Ihrer Zugänge knacken, oder? Notieren Sie Passwörter niemals auf Klebezetteln oder in unverschlüsselten Dateien.

02.

LÄNGERE PASSWÖRTER SIND BESSERE PASSWÖRTER

Zum Schutz vor Brute Force-Angriffen empfiehlt das NIST (National Institute for Standards and Technology) Passwörter mit einer Länge von mindestens acht Zeichen.

03.

UNSER LIEBLING: PASSPHRASEN

Eine Phrase mit mindestens 30 Zeichen, selbst wenn sie nur aus Buchstaben besteht, ist wesentlich sicherer als ein 8-Zeichen-Passwort mit den typischen Ersetzungen (z.B. „3“ für „e“, „!“ für „i“ oder „l“ usw.). Phrasen lassen sich auch viel leichter merken, die zusätzliche Länge stört also kaum.

04.

VERGESSEN SIE KOMPLIZIERTE REGELN

Groß- und Kleinbuchstaben, mindestens eine Zahl und ein Sonderzeichen ... So verleiten Sie Nutzer eher dazu, immer dieselben Passwörter zu verwenden oder haben ständig Ärger mit vergessenen Passwörtern.

05.

BEHALTEN SIE IHRE PASSWÖRTER FÜR SICH

Kriminelle geben sich gern als Bekannte aus, deshalb gilt: Ihre Passwörter gehen niemanden etwas an, weder Ihre Kollegen noch Ihre Familie, Ihre Vorgesetzten oder Support-Mitarbeiter.

06.

„TYPISCHE“ ZEICHENFOLGEN? KEINE GUTE IDEE

So verlockend es auch sein mag: „XXXX“ ist kein starkes Passwort, genauso wenig Zeichenfolgen wie „1234“, „abcd“ oder „qwertz“.

07.

WÖRTERBUCH-EINTRÄGE? NEIN, DANKE

Auch Angreifer arbeiten mit Wörterbüchern und können solche Passwörter relativ einfach per Brute Force knacken. Auch Fremdsprachen- oder Fachwörterbücher sind natürlich keine gute Idee.

08.

AUCH ANDERE KENNEN IHREN SPITZNAMEN (UND ANDERE PERSÖNLICHE DATEN)

Soziale Medien wissen alles, im Zweifel auch Ihren Geburtstag, den Namen Ihres Kindes oder Ehepartners, Ihre Adresse oder Ihren zweiten Vornamen. Und mit ihnen die potentiellen Angreifer.



CYBERSECURITY
EXPERTS ON YOUR SIDE

Für mehr Informationen besuchen Sie:
[ESET.DE](https://www.eset.de) | [ESET.AT](https://www.eset.at) | [ESET.CH](https://www.eset.ch)