Na sicher...

✔ Sichere Passwörter

EIN SICHERES PASSWORT SOLLTE

- aus mindestens 8, am besten 20 Zeichen bestehen,
- Buchstaben, Zahlen und Sonderzeichen enthalten,
- im Idealfall keinerlei Bedeutung haben, sondern rein zufällig gewählt sein.

SO KREIERT MAN EIN SICHERES PASSWORT, DAS MAN SICH AUSSERDEM NOCH GUT MERKEN KANN:

Man denkt sich einen Satz aus (oder nimmt ihn aus einem Buch). Dann nimmt man jeweils die ersten Buchstaben der Wörter, zusammen mit den Satzzeichen.
Beispielsatz: **S**ag **m**al**, k**ommst **d**u **u**m **19 U**hr **z**u **L**ena**?**
Passwort: **Sm,kdu19UzL?**

✕ Unsichere Passwörter

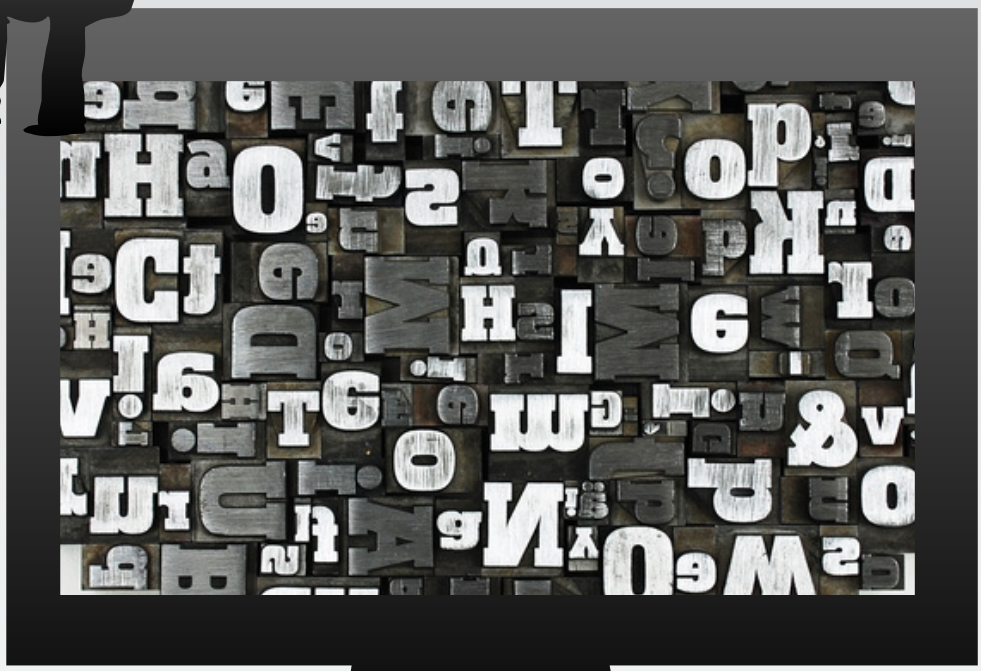
SO BELIEBT WIE UNSICHER SIND SOLCHE PASSWÖRTER:

- Buchstabenfolgen der Computertastatur, z.B. asdf
- einfache Zahlenketten wie 12345, 54321 oder 12121
- Eigennamen
- Geburtstage, Geburtsjahre usw.
- Wörter wie „Passwort" oder „geheim"

HACKER-METHODEN

Passwörter werden meisten mit der Brute-Force-Methode geknackt. Dabei spielt ein Computerprogramm mögliche Zeichenkombinationen durch. Beim Wörterbuchangriff werden dafür nur Begriffe aus einem Wörterbuch benutzt. Man kann sich also unschwer vorstellen: Je mehr zufällig gewählte Zeichen man für sein Passwort benutzt, desto schwerer haben es die Hacker.

Beispiel:
Ein Passwort, das aus vier kleingeschriebenen Buchstaben besteht, hat ein Hacker mit der Brute-Force-Methode in einer Sekunde geknackt.
Für ein Passwort mit zehn Buchstaben braucht er zwei Tage.
Und wenn die zehn Buchstaben teils groß, teils klein geschrieben sind, dauert es fünf Jahre, das Passwort zu knacken!



Ein sicheres Passwort zu wählen, ist nur die halbe Miete. Wichtig ist außerdem:

Passwörter geheim halten und nicht aufschreiben.

Jedes Passwort nur einmal benutzen.

Passwörter unbedingt regelmäßig ändern.

Microsoft