

# LEITFADEN FÜR SICHERE PASSWÖRTER

## Eigenschaften von sicheren Passwörtern

- ✔ Komplexe Passwörter
- ✔ Individuelle Passwörter für jede Website und Software.
- ✔ Groß- und Kleinbuchstaben
- ✔ Sonderzeichen
- ✔ Mindestens 12 Zeichen
- ✔ Passwörter aus Sätzen oder einfach zu merkenden Texten
- ✔ (Sprichwörter, Songtexte)
- ✔ Passwortmanager verwenden

## Unsichere Passwörter

- ✘ Einfache Passwörter
- ✘ Kurze Passwörter
- ✘ Mehrfachverwendung von Passwörtern
- ✘ Persönliche Informationen
- ✘ Sonderzeichen
- ✘ Passwörter öffentlich auf Post-Its oder unter der Tastatur
- ✘ Kennwörtern mit Kollegen teilen
- ✘ **#Start22!#** ist definitiv kein gutes Passwort!



## Wie bildet / generiert man gute, sichere Passwörter?

1. Man denkt sich einen Satz mit mindesten 11 Wörtern aus, der auch mind. eine Zahl enthält.
2. Jeweils den ersten Buchstaben jedes Wortes inkl. der Zahl verwenden und daraus das Passwort erstellen.
3. Sonderzeichen ergänzen

**Beispielsatz:** Am Sonntag um 10 Uhr freue ich mich auf den köstlichen Marmeladentoast mit Ei!

Das daraus gebildete Passwort:

**ASu10UfimadkMmE!**

