Kurzanleitung – Sichere Erstellung von Passwörtern

So erstellt man ein gutes Passwort

Ein gutes Passwort soll sicher sein, aber trotzdem noch merkbar bleiben.

Voraussetzungen eines sicheren Passworts

Ein Passwort sollte:

- **mindestens 14 Zeichen lang** sein,
- mindestens **einen Großbuchstaben** enthalten,
- mindestens **einen Kleinbuchstaben** enthalten,
- mindestens **eine Zahl** enthalten,
- mindestens **ein Sonderzeichen** enthalten, zum Beispiel !, ?, # oder %.

Keine einfachen Passwörter verwenden

Nicht erlaubt sind Passwörter, die leicht zu erraten sind, zum Beispiel:

- Vorname + Geburtsdatum
- Name der Schule
- Monate oder Jahreszeiten mit Jahreszahl
- einfache Wörter wie Passwort123

Für jedes Konto ein eigenes Passwort

- Ein Passwort darf **nicht für mehrere Konten gleichzeitig** verwendet werden.
- Jedes System und jede Anwendung sollte ein **eigenes Passwort** haben.

Passwörter sollen merkbar sein

- Ein Passwort darf sicher sein, soll aber nicht so kompliziert sein, dass man es sofort wieder vergisst.
- Gut geeignet sind **Passphrasen**, also mehrere Wörter in einer Folge.

!	**Beispiel für eine gute Passphrase:** ***SonneFahrradPizza8!*** Solche Passwörter sind oft leichter zu merken und trotzdem sicher.

Passwort ändern

- Das Passwort kann in der Regel jederzeit geändert werden.
- Bei jeder Änderung sollen die genannten Regeln beachtet werden.

Regeln eines sicheren Passwortgebrauchs:

Damit Konten und persönliche Daten geschützt bleiben, ist ein sicheres Passwort sehr wichtig. Die folgenden Regeln helfen dabei.

1. **Passwort geheim halten**
2. **Alte Passwörter nicht weiterverwenden**
3. **Passwort sofort ändern, wenn etwas auffällig ist**
4. **Passwort immer unbeobachtet eingeben**
5. **Startpasswörter sofort ändern**
6. **Passwort nicht sichtbar speichern**
7. **Zwei-Faktor-Anmeldung nutzen**
8. **Andere Zugangsmittel ebenfalls schützen**
9. **Verlust sofort melden**