Anleitung: Sicherer Umgang mit Passwörtern

Viele Online-Dienste benötigen ein eigenes Benutzerkonto. Damit eure Daten und Zugänge geschützt bleiben, solltet ihr einige grundlegende Regeln für sichere Passwörter beachten.

Grundregeln für sichere Passwörter

- Für **jeden Dienst ein eigenes Passwort** verwenden
- **Lange Passwörter** nutzen (mindestens 12–16 Zeichen)
- Eine Mischung aus **Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen**
- **Keine persönlichen Daten** verwenden (Name, Geburtstag, Verein, etc.)
- Passwörter **nicht per E-Mail oder Messenger weitergeben**
- Passwörter **regelmäßig ändern**, besonders wenn ein Dienst kompromittiert wurde

Beispiel für gute Passwörter

Statt einfacher Passwörter wie:

```
passwort123
sand2024
```

besser sogenannte **Passphrasen** nutzen, z.B.:

```
Apfel!Mond!Koffer!2026
Theater!Probe!Licht!Buehne
```

Diese sind deutlich schwerer zu erraten und trotzdem gut merkbar.

Problem: Zu viele Passwörter

Da man für jeden Dienst ein eigenes Passwort verwenden sollte, wird es schnell schwierig, sich alle zu merken.

Die Lösung dafür ist ein **Passwortmanager**.

Was ist ein Passwortmanager?

Ein Passwortmanager ist ein Programm oder eine App, die:

- alle Passwörter **verschlüsselt speichert**
- **starke Passwörter automatisch generiert**
- Passwörter **automatisch ausfüllt**

- auf **Computer, Smartphone und Tablet synchronisiert**

Ihr müsst euch dann nur noch **ein einziges starkes Master-Passwort** merken.

Empfohlene Passwortmanager

Kostenlose Lösung

Ein sehr guter kostenloser Passwortmanager ist:

- Bitwarden

Vorteile:

- kostenlos nutzbar
- Open Source
- Apps für Windows, Mac, Linux, Android und iOS
- Browser-Erweiterungen für Chrome, Firefox, Edge usw.
- Synchronisation zwischen allen Geräten

Kostenpflichtige Alternativen

Einige Anbieter bieten Passwortmanager als Teil eines größeren Sicherheits-Pakets an.

Beispiele:

- NordPass von der Firma (bekannt durch den Dienst)
- 1Password
- Dashlane

Diese bieten häufig zusätzliche Funktionen wie:

- Sicherheitsüberprüfung der Passwörter
- Warnung bei Datenlecks
- Familien- oder Teamzugänge

Tipps zur Nutzung eines Passwortmanagers

- Wählt ein **sehr starkes Master-Passwort**
- Aktiviert wenn möglich **2-Faktor-Authentifizierung (2FA)**
- Speichert **alle neuen Passwörter direkt im Manager**
- Nutzt die **Passwortgenerator-Funktion**

Fazit

Ein Passwortmanager erhöht die Sicherheit deutlich und erleichtert gleichzeitig den Umgang mit vielen Online-Konten.

Gerade bei Vereins- oder Projektarbeit hilft er dabei, Zugänge sicher zu verwalten und Daten zu schützen.

Zurück zu Wissen (Start).

From:
https://www.wiki.theatergruppe-sand.de/ - **wiki.theatergruppe-sand.de**

Permanent link:
https://www.wiki.theatergruppe-sand.de/doku.php?id=wissen:howtos

Last update: **2026/03/11 16:44**