

Passwörter und Benutzerkonten

- [2.1 Warum Passwörter wichtig sind](#)
- [2.2 Ein gutes Passwort](#)
- [2.3 Passwortmanager](#)
- [2.4 Passwörter niemals weitergeben](#)
- [2.5 Was tun bei Verdacht auf ein gestohlenes Passwort?](#)

2.1 Warum Passwörter wichtig sind

Ein Passwort schützt den Zugang zu einem Benutzerkonto. Wer das Passwort kennt, kann gegenüber einem System möglicherweise so auftreten, als wäre er der eigentliche Benutzer.

Vergleich aus dem Alltag

Ein Passwort ist wie ein persönlicher Schlüssel. Wer eine Kopie besitzt, kann versuchen, dieselbe Tür zu öffnen.

Beispiel aus dem Arbeitsalltag

Mit einem gestohlenen Passwort könnte ein Angreifer versuchen, auf E-Mail oder andere Dienste zuzugreifen.

“ **Merke:** Passwörter sind geheim und werden nicht an Kollegen weitergegeben.

2.2 Ein gutes Passwort

Gute Passwörter sind vor allem lang und einzigartig. Kurze oder leicht erratbare Wörter sind ungeeignet. Dasselbe Passwort sollte nicht für mehrere wichtige Konten verwendet werden.

Vergleich aus dem Alltag

Wenn ein Schlüssel für Haus, Auto und Firma passt, ist sein Verlust besonders schlimm.

Beispiel aus dem Arbeitsalltag

Gerät ein Passwort eines fremden Onlineshops in falsche Hände, darf dieses Passwort nicht gleichzeitig das Firmenkonto öffnen.

Passwörter: lang und einzigartig

Schlecht

kurz · wiederverwendet
leicht zu erraten

Besser

lang · einzigartig
im Passwortmanager

“ **Merke:** Lang und einzigartig ist wichtiger als ein möglichst kompliziert aussehendes kurzes Passwort.

2.3 Passwortmanager

Ein Passwortmanager kann für verschiedene Konten unterschiedliche starke Passwörter speichern und erzeugen. Dadurch muss man sich nicht jedes einzelne Passwort merken.

Vergleich aus dem Alltag

Ein Passwortmanager ist wie ein gut geschützter Schlüsseltresor.

Beispiel aus dem Arbeitsalltag

Statt dasselbe Passwort an zehn Stellen zu verwenden, erzeugt der Passwortmanager zehn unterschiedliche Kennwörter.

“ **Merke:** Passwortmanager erleichtern sichere, einzigartige Passwörter.

2.4 Passwörter niemals weitergeben

Ein persönliches Passwort gehört ausschließlich zum eigenen Konto. Auch die IT sollte dein normales persönliches Kennwort nicht benötigen, um ein technisches Problem zu untersuchen.

Vergleich aus dem Alltag

Ein Techniker braucht für eine Reparatur nicht automatisch deinen persönlichen Haustürschlüssel für immer.

Beispiel aus dem Arbeitsalltag

Fordert jemand per Telefon oder E-Mail dein Passwort an, ist das ein Warnzeichen.

“ **Merke:** Persönliche Passwörter werden nicht per E-Mail, Chat oder Telefon weitergegeben.

2.5 Was tun bei Verdacht auf ein gestohlenes Passwort?

Wenn du glaubst, dass jemand dein Passwort kennt, zählt Zeit. Informiere die IT und ändere das betroffene Passwort nach den vorgesehenen Verfahren. Verschweige den Verdacht nicht.

Vergleich aus dem Alltag

Wenn ein Haustürschlüssel verschwunden ist, wartet man nicht erst ab, ob eingebrochen wird.

Beispiel aus dem Arbeitsalltag

Du hast dein Kennwort versehentlich auf einer verdächtigen Webseite eingegeben.

Was soll ich tun?

Ein möglicherweise gestohlenes Passwort ist bereits ein Sicherheitsvorfall.

“ **Merke:** IT unverzüglich informieren und den Vorfall genau beschreiben.