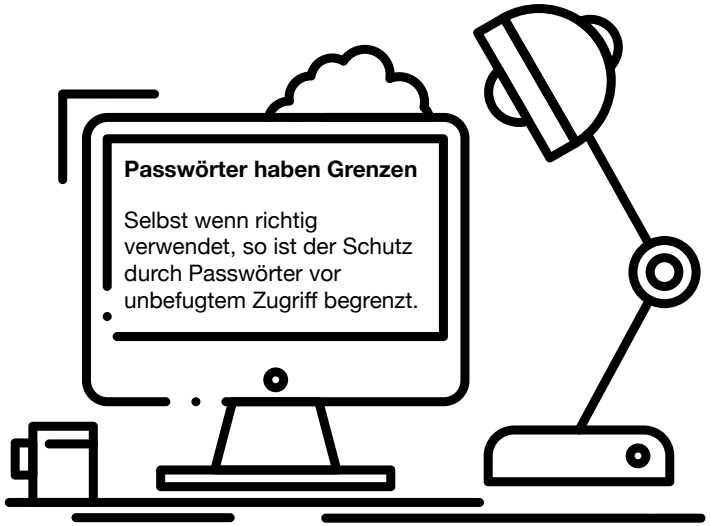
# Passwörter & Zugriffsschutz

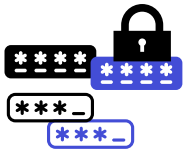
Wie sicher personenbezogene Daten auf unseren digitalen Endgeräten, in Programmen bzw. Apps und Online-Plattformen sind, hängt maßgeblich davon ab, wie gut wir den Zugang dazu schützen. Mit welchen Gefahren müssen Nutzer rechnen, wenn es um den Zugriffsschutz auf personenbezogene Daten geht und wie kann der Schutz verbessert werden?

## Wie Passwörter entdeckt werden …

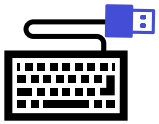
**Ausspähen**
Passwörter können bei der Eingabe durch Blick auf die Tastatur mitgelesen werden.

**Diebstahl**
Werden Passwörter unsicher verwahrt, können sie entwendet werden.



**Passwort Spraying**
Eine kleine Zahl häufig verwendeter Passwörter wird genutzt, um Zugriff auf viele Konten zu erhalten.

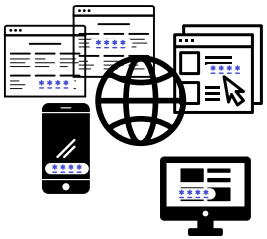


**Key-Logging**
Passwörter werden bei der Eingabe durch Software (z.B. Trojaner) oder Hardware (z.B. USB Key Logger) ausgelesen.

**Erraten**
Passwörter lassen sich erraten, wenn Geburtstage, Namen von Kindern und Haustieren oder ähnlich genutzt werden. Selbiges gilt auch für Sicherheitsfragen zur Wiederherstellung von Passwörtern.

**Wörterbuch Attacken**
Hacker versuchen Logins mit Wörtern aus umfangreichen Wörterbüchern.

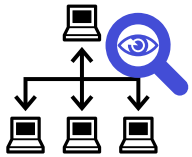
**Server Hack**
Durch Angriff auf einen Server werden Zugangsdaten vieler Nutzer gestohlen.



**Wiederverwendung**
Hacker testen erbeutete Zugangsdaten an anderen Systemen & Online-Plattformen.

**Phishing**
Nutzer werden durch Tricks dazu gebracht, Passwörter preiszugeben.

**Brachial Attacken**
Hacker testen Milliarden von Zufalls-Passwörtern an Online-Portalen und Systemen durch.



**Abfangen**
Passwörter können abgefangen werden, wenn sie durch das Netz reisen.

# … und wie man die Sicherheit verbessern kann.

**Alternative Authentifizierung**
Wo Systeme, Apps und Online-Plattformen es zulassen, sollten alternative Anmeldungsverfahren wie Fingerabdruck, Security Key, OTP Dongle oder Authenticator App* eingerichtet werden.

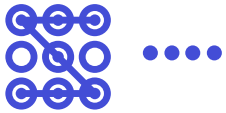
**Passwörter nur 1x nutzen**
Für verschiedene Systeme, Apps und Online-Plattformen sollten nie gleiche Passwörter verwendet werden. Auch verschiedene Konten in einer Plattform (z.B. Admin, Lehrer) sollten nie gleiche Passwörter haben.

**Öffentliche WLAN Hotspots**
Keine Logins von unsicheren WLAN Zugängen aus, um das Abfangen von Passwörtern zu vermeiden.

**2-Faktor-Authentifizierung (2FA)**
Besonders kritische Systeme, Anwendungen und Online-Plattformen sollten mit einer zusätzlichen Geheimnisabfrage geschützt werden, z.B. Security Key, Authenticator App, OTP Dongle*.

**Passwörter nicht nutzen, wo sie ausgespäht werden können**
An Orten, wo Passworte durch Ausspähen gefährdet sind (z.B. im Klassenraum), sollte man eine alternative Authentifizierung nutzen, wie Fingerabdruck oder Security Key.

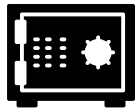
**Überall sichere Passwörter**
Alle Passwörter sollten sicher sein, vor allem aber bei Plattformen, über welche Zugänge zu anderen Plattformen wiederhergestellt werden können, z.B. E-Mail Konten.



**Unsichere alternative Authentifizierung vermeiden**
Kurze numerische Pin Codes und Entsperrmuster sind bequem aber höchst unsicher. Sie sollten nicht genutzt werden, wo es um kritische Daten geht oder eine Möglichkeit besteht, über Umwege die Sicherheit anderer Zugänge zu gefährden.

**Bei Sicherheitsfragen LÜGEN!**
Sicherheitsfragen zur Passwortwiederherstellung fragen oft Dinge ab, die Dritte leicht erraten oder ermitteln können. Deshalb immer Fantasieantworten geben, die im Passwortmanager hinterlegt werden.

**Unsichere Rechner meiden!**
Ein Login von öffentlichen PC gefährdet die Sicherheit von Zugängen.



**Schutz für Passwörter**
Durch Passwortmanager wie KeyPass, LastPass, 1 Password u. Ä. lassen sich große Mengen von Passwörtern sicher verwahren und nutzen.

**Sichere Passwörter**
Bei der Erstellung von sicheren Passwörtern nutzt man einen Passwortmanager zur Passworterzeugung oder orientiert sich an der Richtlinie des BSI für sichere Passwörter.


**URL checken**
Bei Websites und Online-Plattformen immer die URL vor dem Login prüfen. Bei Links von verdächtigen externen Quellen (z.B. E-Mail, Dokument, Website) zur Sicherheit die URL von Hand eingeben.

*__OTP Dongle__ = One Time Passwort Dongle, erzeugt auf Knopfdruck Einmalpasswörter; __Authenticator App__ = erzeugt Einmalpasswörter; __Security Key__ = ein USB Dongle, der eine gesicherte Authentifizierung ermöglicht.

Siehe auch **BSI Passwörter**