

SICHERE PASSWÖRTER – SO GEHT'S RICHTIG

1 Gute und sichere Passwörter

Ein sicheres Passwort sollte ...

- mindestens 12 Zeichen lang sein.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.
- keine persönlichen Daten, wie Name, Geburtsdatum oder Wohnort enthalten.
- nicht aus einfachen Worten oder Tastaturmustern bestehen (z. B. „123456“, „Passwort“, „qwertz“).



Ein sicheres Passwort ist wie ein starker Schlüssel. Es schützt deine Daten!

3 Beste Praxis

Nutze ein Passwort immer nur für ein Konto/ Seite/ Dienste.

Wenn dir vom (Online-)Dienst ein **Passkey** oder die **Multifaktor-Authentifizierung** angeboten wird, kannst du diese ruhig nutzen. Es unterstützt deine Sicherheit.



4 Sicherheit

Gib dein Passwort NICHT weiter.


Wenn du dein Passwort aufschreibst, lassen es nicht für andere offen liegen.



5 Passwortmanager: Dein digitaler Tresor

Der Passwortmanager kann ...

- dir starke und einzigartige Passwörter alle Konten/ Seiten/ Dienste erstellen.
- alle deine Passwörter sicher speichern.


 Du musst dir nur noch ein einziges Passwort merken, das für den Passwortmanager.



6 Tipp!

Bei wichtigen Konten solltest du einmal im Jahr dein Passwort ändern.

Wusstest du schon?

 Am 01. Februar ist der „Ändere-Dein-Passwort-Tag“.

7 Wenn doch mal etwas schief läuft ...

Ändere sofort das Passwort!

Mit deinen Zugängen in der Schule stimmt etwas nicht oder du hast das Gefühl jemand hat dein Passwort geknackt? Informiere sofort eine Lehrkraft.



Begriffserklärung

Ein **Passkey** ist ein digitaler Schlüssel, mit dem du dich sicher und ohne Passwort bei Apps oder Webseiten anmelden kannst.

Multifaktor-Authentifizierung bedeutet, dass du dich mit zwei oder mehr verschiedenen Methoden anmeldest, zum Beispiel mit Passwort und einem Code aufs Handy.