

# Passwörter



## Die 10 beliebtesten Passwörter 2021



# Passwörter



Wer kennt es nicht?

Sie wollen einen Dienst im Internet nutzen,  
und schon wird eine Anmeldung mit Passwort notwendig.

z.B.:

Email Konto

Shops

Onlinebanking

Nachrichten

Spiele

Social Media

Behördenseiten etc.

# *Warum sollten Passwörter schwer zu erraten sein?*



## **Hacker arbeiten mit**

- Werkzeugen/Programmen um Passwörter vollautomatisch auszuprobieren
- ganzen Wörterbüchern und Lexika
- mit gängigen Kombinationen aus Worten und angefügten Zahlen
- Listen von im Internet geklauten bzw. gehandelten Zugangsdaten
- schnellen Rechnern und künstlicher Intelligenz

# Der Weg zu sicheren Passwörtern



## BSI empfiehlt:

(Bundesamt für Sicherheit in der Informationstechnik)

## 2 verschiedene Strategien für sichere Passwörter

### 1. lang und weniger komplex

- min 25 Zeichen aus 2 Zeichenarten (z.B. Groß- und Kleinbuchstaben, oder Buchstaben und Sonderzeichen oder Buchstaben und Ziffern)
- z.B.: tisch\_hund\_lila\_moped\_mondschein

### 2. kürzer und komplexer

- 8 - 12 Zeichen aus 4 Zeichenarten (Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen)
- z.B.: 8v&hQhZ(

# Weitere Tipps



- Verwenden Sie für jedes Konto ein anderes Passwort
- Nutzen Sie, wenn möglich, die Zwei-Faktor-Authentisierung
- Benutzen Sie alle 4 Zeichenarten
  - Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen
  - Vorsicht mit sprachspezifischen Zeichen (äöü, ÄÖÜ, € etc.)

## Vermeiden Sie

- Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster (z.B.: asdfgh, qwertz, 1234abcd)
- Einfach nur Ziffern oder Sonderzeichen an den Anfang oder das Ende eines einfachen Passwort anzufügen

# Passwörter



- niemals **unverschlüsselt** auf dem PC speichern!
- niemals an Dritte weitergeben!
- niemals per Email verschicken!
- nie auf einen Zettel unter die Tastatur oder an den Bildschirmrand kleben!
- voreingestellte Passwörter **immer** ändern!
- sofort ändern, wenn der Verdacht besteht, dass das Passwort Unberechtigten bekannt ist!

# Passwörter merken, aber wie?

## Teil I



*Es gibt verschiedene Tricks. Hier zwei Möglichkeiten.*

- *einen Satz ausdenken und von jedem Wort nur den 1. Buchstaben benutzen. Dann bestimmte Buchstaben durch Zahlen oder Sonderzeichen ersetzen. z.B.:*
  - *Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang. ==> MsiaupmmZdMI*
  - *"i und l" sieht aus wie "1", "&" ersetzt "und": Ms1a&pmmZ3M1*
  - *Den Satz selber ausdenken.  
Keine bekannten Zitate aus der Literatur verwenden*

# Passwörter merken, aber wie?

## Teil II



- *Passworte zweiteilen*
  - 1. Teil des Passwortes merken. Ist immer gleich.
  - 2. Teil des Passwortes immer anders.
  - den 2. Teil in ein Merkblatt eintragen

### 1. Teil des Passworts merken



- Für jeden Account gleich
- Ohne persönlichen Bezug
- Mindestens acht Zeichen lang
- Besteht bspw. aus zwei ausgedachten, aneinander gereihten Wörtern  
(tisch-himmel)

### 2. Teil des Passworts in Liste eintragen



- Für jeden Account anders
- Entweder kurz und komplex oder besonders lang
- Besteht bspw. aus willkürlich aneinander gereihten Zeichen oder aus vier Wörtern, die durch Sonderzeichen getrennt sind  
(Berg\_spät\_hüpfen\_Kühlschrank)




### Sichere Passwörter für jeden Account

(tisch-himmelBerg\_spät\_hüpfen\_Kühlschrank)

Account	Nutzername/ E-Mail-Adresse	2. Teil des Passworts
1. Musteraccount	maxine@musterfrau.de	Berg_spät_hüpfen_Kühlschrank
2. Musteraccount	maxine@musterfrau.de	q7yPv8!x\$B2



# Links



- BSI, Bundesamt für Sicherheit in der Informationstechnik
  - [https://www.bsi.bund.de/DE/Home/home\\_node.html](https://www.bsi.bund.de/DE/Home/home_node.html)
  - Sichere Passwörter erstellen
  - Passwörter Schritt-für-Schritt merken
  
- Passwortmanager
  - Passwortmanager: Keepass
  - Stiftung Warentest: Passwort-Manager im Test