

Ein starkes und sicheres Passwort erstellen

Länge ist entscheidend

Bei Passwörtern gilt: Je länger, desto besser.

Ein kurzes Passwort von mindestens 8 Zeichen muss deutlich komplexer aufgebaut sein als ein langes Passwort mit beispielsweise 25 Zeichen.

Ein Passwort mit mindestens 8 Zeichen sollte aus allen vier Zeichenarten bestehen:

- Grossbuchstaben
- Kleinbuchstaben
- Zahlen
- Sonderzeichen (z. B. ! ? * @ \$ %)

Ein Passwort mit 25 Zeichen oder mehr kann auch mit nur zwei Zeichenarten sicher sein, da die Länge den Schutz erheblich erhöht.

Merkbarkeit durch Eselsbrücken

Ein gutes Passwort muss nicht nur sicher, sondern auch merkbar sein. Hilfreich ist die Methode, sich einen Satz auszudenken und von jedem Wort den Anfangsbuchstaben zu verwenden.

Beispiel:

„Hans isst gerne Spaghetti mit Ketchup zum Mittag.“

→ HigSmKzM

Erweitert man den Satz durch Zahlen und Sonderzeichen, wird das Passwort noch sicherer:

„Hans isst gerne 2x Spaghetti mit Ketchup zum Mittag!“

→ Hig2xSmKzM!

So merkt man sich lediglich den Satz, nicht die zufällige Zeichenfolge.

Keine persönlichen Daten

Ein Passwort sollte niemals persönlichen Bezug zu dir haben. Dazu zählen:

- Vor- oder Nachnamen
- Geburtsdaten
- Namen von Familienmitgliedern oder Haustieren
- Hobbys oder Wohnort

Ein Passwort wie *Hans2508?* ist für Angreifer leicht zu erraten, weil solche Daten oft öffentlich zugänglich oder naheliegend sind.

Keine Muster oder Wiederholungen

Vermeide einfache Tastaturmuster oder Zeichenfolgen wie:

- „123456...“
- „abcdef...“
- „asdfgh...“
- Wiederholungen wie „aaaa1111“

Solche Passwörter können in Sekunden geknackt werden.

Sonderzeichen richtig einsetzen

Es reicht nicht, nur am Anfang oder Ende ein Sonderzeichen hinzuzufügen, wie in:
*HigSmKzM**

Stattdessen sollten Sonderzeichen innerhalb des Passworts platziert werden:
Hi#gSmK!zM2

Keine Passwort-Wiederverwendung

Wiederverwende niemals das gleiche Passwort für mehrere Konten oder Portale.
Wenn ein Anbieter gehackt wird, sind sonst alle deine anderen Konten sofort gefährdet.

Tipps:

Passwort-Manager nutzen

Da sich lange und komplexe Passwörter nur schwer merken lassen, empfiehlt es sich, einen Passwort-Manager (z. B. Bitwarden, 1Password, KeePass) zu verwenden. Dieser speichert deine Passwörter sicher, sodass du dir nur ein einziges starkes Master-Passwort merken musst.

Passwortcheck.ch

Mithilfe von Passwortcheck kann man herausfinden, wie lange es dauert, bis jemand ein Passwort knacken kann. Es zeigt ausserdem an, wie stark ein Passwort ist.

Das zu prüfende Passwort lautet:

☐ **Passwort anzeigen**
Das eingegebene Passwort wird lokal überprüft und nie an den Server übermittelt.

Das Passwort ist **Stark**, weil die geschätzte Zeit für die Suche über einem Jahr ist.

Ausgewählte Wörterbücher

☒ **Deutsch**☐ Französisch☐ Italienisch
☐ Rätoromanisch☒ **Englisch**

Teilwörter	Länge	Typ	Raumgrösse	Anzahl Versuche	Entropie	Rechenzeit
***	11	Übrige Zeichen	102	1.243e+22	73 Bit	
Aufwandschätzung				1.243e+22	73 Bit	3'943 Jahre

Fazit:

Ein starkes Passwort ist **lang, einzigartig, komplex und merkbar, aber ohne persönlichen Bezug.**

Bei Fragen oder Problemen stehen wir gerne unter [+41 27 510 50 95](tel:+41275105095) oder itsupport@furmica.ch zur Verfügung.