

Sichere Passwörter – Grundlagen und Praxisbeispiele

1. Warum sind “sichere” Passwörter wichtig?

Passwörter schützen unsere persönlichen Daten und verhindern den unbefugten Zugriff auf Konten und Systeme. Unsichere Passwörter ermöglichen es Angreifern, durch sogenannte „Brute-Force“-Attacken oder Phishing leichter an sensible Informationen zu gelangen. Ein starkes Passwort ist der erste Schritt zur Cybersicherheit.

Beispiel:

Ein unsicheres Passwort wie „123456“ oder „passwort“ kann in Sekunden von Angreifern geknackt werden. Ein sicheres Passwort hingegen kann Jahrzehnte dauern, bis es entschlüsselt wird.

2. Merkmale eines sicheren Passworts

Ein sicheres Passwort sollte:

- Mindestens 12 Zeichen lang sein.
- Groß- und Kleinbuchstaben enthalten.
- Zahlen und Sonderzeichen (z.B. !, \$, %, &) beinhalten.
- Nicht auf persönlichen Informationen wie Geburtsdatum oder Namen basieren.
- Nicht auf häufig verwendeten Wörtern, Tastaturmustern oder Wiederholungen beruhen.
-

Beispiel für ein sicheres Passwort:

- Unsicheres Passwort: „Passwort123“
- Sicheres Passwort: „aS!9d2G\$7mK&“

3. Wie erstellt man ein sicheres Passwort?

Methode 1: Zufällige Zeichenkombination

Ein völlig zufällig generiertes Passwort ist am sichersten, da es keinem Muster folgt.

Beispiel:

„T7g#Yd!3kLm&92“

Zufällige Passwörter können durch Passwort-Manager wie KeePass oder LastPass generiert und sicher gespeichert werden.

Methode 2: Passphrasen

Eine Passphrase besteht aus einer Reihe von Wörtern, die in einer bestimmten Reihenfolge stehen. Passphrasen sind oft leichter zu merken, aber trotzdem sicher.

Beispiel:

„KaffeeBuchHund!Pizza2024?“

Diese Methode ist besonders nützlich, da sie einfach zu merken, aber schwer zu erraten ist.

Methode 3: Kombination persönlicher Regeln

Man kann eine persönliche Regel verwenden, um ein Passwort zu erstellen, das für andere schwer nachvollziehbar ist.

Beispiel:

Verwende das erste Buchstaben jedes Wortes eines leicht zu merkenden Satzes.

Satz: „Mein Lieblingsfilm ist Inception und ich schaue ihn 3 Mal im Jahr!“

Passwort: „MLfiluisih3Mij!“

4. Häufige Fehler bei Passwörtern

Wiederverwendung von Passwörtern: Wenn du dasselbe Passwort für mehrere Konten nutzt, kann ein gehacktes Konto leicht zum Verlust aller Konten führen. Kurze oder einfache Passwörter: Passwörter unter 8 Zeichen sind sehr unsicher. Passwörter ohne Sonderzeichen: Vermeide Passwörter, die nur Buchstaben und Zahlen enthalten, da sie leichter zu knacken sind.

Beispiel:

- Unsicheres Passwort: „Sommer2024“
- Sicheres Passwort: „S0m!2024M\$r!“

5. Praktische Tipps für den Umgang mit Passwörtern

1. Nutze einen Passwort-Manager

Passwort-Manager wie 1Password, LastPass oder KeePass helfen dabei, sichere Passwörter zu generieren und sicher zu speichern. Du brauchst dir dann nur noch ein „Master-Passwort“ zu merken.

2. Aktiviere die Zwei-Faktor-Authentifizierung (2FA)

Selbst ein starkes Passwort ist keine vollständige Garantie. Mit 2FA fügst du eine zweite Sicherheitsebene hinzu, z.B. durch einen Code auf deinem Smartphone.

3. Ändere Passwörter regelmäßig

Ändere wichtige Passwörter regelmäßig, besonders wenn du den Verdacht hast, dass ein Konto kompromittiert wurde.

6. Beispiele aus der Praxis: Passwort-Hacks

LinkedIn-Datenleck (2012): Millionen von Passwörtern wurden gestohlen, viele davon waren leicht zu erraten (z.B. „123456“, „password“). Adobe-Datenleck (2013): 153 Millionen Passwörter wurden durchgesickert, und „123456“ war eines der häufigsten. Diese Vorfälle zeigen die Gefahr unsicherer Passwörter und die Notwendigkeit, auf starke Sicherheitsmaßnahmen zu setzen.

7. NICHT VERGESSEN:

- Länge und Komplexität sind entscheidend für sichere Passwörter.
- Nutze Passwort-Manager und Zwei-Faktor-Authentifizierung.
- Vermeide häufige Fehler wie Passwortwiederverwendung.
- Ändere wichtige Passwörter regelmäßig, besonders wenn ein Verdacht auf einen Sicherheitsvorfall besteht.