Sichere Passwörter erstellen

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Einleitung 3
Technischer Hintergrund 4
Warum moderne Passwörter komplex sind 5
Wiederverwendung vermeiden 6
Wie erstellt man ein sicheres Passwort 7
Zusätzliche Tipps und Tricks 9

Einleitung

Ein Passwort schützt den Zugang zu Mailkonto, Bankkonto, Fotos, Einkäufen und privaten Daten. Wer dein Passwort kennt, erhält Zugriff auf deinen persönlichen Daten.

Früher waren Passwörter oft kurz. Ein Name oder eine vierstellige Zahl hat gereicht. Das hat nur funktioniert, weil es weniger Onlinekonten, weniger Datenlecks und weniger automatische Angriffe gab.

Heute testen automatisierte Angriffsprogramme Passwörter systematisch. Bekannte und unbekannte Tools wie Brute-Force-, Dictionary-, Credential-Stuffing- oder Botnet-Angriffe sind darauf ausgelegt, online automatisiert Angriffe durchzuführen und viele mögliche Kombinationen zu testen. Sie verwenden Listen mit häufigen Passwörtern und nutzen geleakte Zugangsdaten aus früheren Hacks.

Das National Institute of Standards and Technology (NIST) entwickelt Standards und Richtlinien mit Fokus auf IT, Sicherheit und Technik und gehört zum US-Handelsministerium. In der Schweiz übernimmt das Nationales Zentrum für Cybersicherheit (NCSC) die Rolle einer zentralen Stelle für IT-Sicherheitsrichtlinien und Empfehlungen.

Das NIST und das NCSC empfehlen einen klaren und praxisnahen Umgang mit Passwörtern. Im Mittelpunkt steht die Länge. Ein Passwort soll ausreichend lang sein, idealerweise mindestens 12 Zeichen, für wichtige Konten deutlich mehr. Je länger ein Passwort ist, desto schwerer lässt es sich automatisiert knacken.

Beide Institutionen betonen, dass jedes Konto ein eigenes Passwort haben muss. Wird ein Passwort mehrfach genutzt, reicht ein einzelner Datenleck, um mehrere Konten zu gefährden. Einzigartige Passwörter pro Dienst sind daher Pflicht.

Komplexe und schwer merkbare Regeln stehen nicht mehr im Fokus. Stattdessen empfehlen beide Stellen einfache, lange Passphrasen, die aus mehreren Wörtern bestehen. Diese sind leichter zu merken und gleichzeitig sicher. Persönliche Informationen wie Namen oder Geburtsdaten sollen nicht enthalten sein.

Ein weiterer zentraler Punkt ist der Einsatz eines Passwort Managers. Damit lassen sich starke, zufällige Passwörter für jeden Dienst erstellen und sicher speichern. Ergänzend soll die Zwei Faktor Authentifizierung aktiviert werden, um den Zugriff zusätzlich abzusichern.

Passwörter sollen nicht regelmässig ohne Grund geändert werden. Eine Änderung ist dann sinnvoll, wenn ein Sicherheitsvorfall vorliegt oder der Verdacht besteht, dass ein Passwort kompromittiert wurde.

Technischer Hintergrund

Ein Bot ist ein automatisches Programm. Es testet Passwörter systematisch und deutlich schneller als ein Mensch.

Bei einem normalen Login begrenzt eine Webseite die Anzahl falscher Versuche. Das bremst Angriffe. Typisch sind Sperren nach mehreren Fehlversuchen oder zusätzliche Prüfungen.

Nach einem Datenleck ändert sich die Situation. Angreifer erhalten oft gespeicherte Prüfwerte von Passwörtern. Diese heissen «Hashes». Sie testen mögliche Passwörter auf eigenen Systemen, ohne die Webseite zu kontaktieren. Diese Angriffe laufen offline und sind nicht begrenzt.

Das National Institute of Standards and Technology und das Nationales Zentrum für Cybersicherheit weisen darauf hin, dass moderne Hardware extrem viele Versuche pro Sekunde durchführen kann. Einfache Passwörter wie 123456, Passwort oder Sommer2026! werden dadurch oft sofort erkannt.

Typische Reihenfolge bei Angriffen

- bekannte geleakte Passwörter
- einfache Zahlenfolgen wie 123456
- Wörter aus Wörterbüchern
- Namen und häufige Begriffe
- Haustiernamen
- Geburtsdaten
- Tastaturmuster wie qwertz
- typische Varianten wie Sommer2026! oder Passwort123!

Programme kombinieren diese Muster automatisch. Sie ersetzen Zeichen, variieren Gross und Kleinschreibung und testen bekannte Strukturen gezielt.

Warum moderne Passwörter komplex sind

Viele Webseiten verlangen Gross und Kleinbuchstaben, Zahlen und Sonderzeichen. Der Grund liegt in der Anzahl möglicher Kombinationen. Je mehr unterschiedliche Zeichenarten ein Passwort enthält, desto grösser wird der Suchraum für Angreifer. Ein automatisiertes Angriffsprogramm muss dadurch deutlich mehr Varianten testen, was den Aufwand stark erhöht.

Beispiel:

Schlecht	Besser	Noch besser
sommer	Sommer7432!	Rigi!7432Tulipe

Ein einfaches Passwort wie «sommer» ist unsicher. Es besteht nur aus Kleinbuchstaben, ist kurz und ein häufiges Wort. Solche Passwörter stehen in Wörterlisten und werden bei Dictionary Angriffen oft in Sekunden erkannt. Ein Angreifer muss hier kaum rechnen, das Passwort ist bereits bekannt.

Ein etwas stärkeres Passwort wie «Sommer7432!» erhöht die Sicherheit. Es kombiniert Gross und Kleinbuchstaben, Zahlen und ein Sonderzeichen. Dadurch steigt die Anzahl möglicher Kombinationen deutlich. Solche Passwörter sind nicht mehr direkt in Standardlisten enthalten und benötigen mehr Versuche.

Ein noch besseres Passwort wie «Rigi!7432Tulipe» geht einen Schritt weiter. Es ist länger und kombiniert mehrere Wörter mit Zahlen und Sonderzeichen. Die Länge erhöht die Sicherheit massiv, da die Anzahl möglicher Kombinationen exponentiell wächst. Selbst wenn einzelne Teile erratbar sind, bleibt das gesamte Passwort schwer zu knacken.

Wichtig ist jedoch: Komplexität allein reicht nicht. Die Länge hat den grössten Einfluss auf die Sicherheit. Ein langes Passwort oder eine Passphrase mit mehreren Wörtern bietet in der Praxis deutlich besseren Schutz als ein kurzes, komplex wirkendes Passwort.

Wiederverwendung vermeiden

Nimm für jedes Konto ein eigenes Passwort. Das NIST und NCSC weisen klar darauf hin, dass wiederverwendete Passwörter eines der grössten Risiken darstellen.

Wenn du dasselbe Passwort mehrfach nutzt, entsteht ein Ketteneffekt.

Schlechtes Beispiel

Mailkonto	Bankkonto	Shopkonto
Sommer2026!	Sommer2026!	Sommer2026!

Hat ein Shop ein Datenleck, testen Angreifer dieses Passwort automatisch bei anderen Diensten. Diese Methode heisst Credential Stuffing. Ein einziges geleaktes Passwort reicht, um mehrere Konten zu übernehmen.

Auch ähnliche Passwörter sind unsicher.

Mailkonto	Bankkonto	Shopkonto
Sommer2024!	Sommer2025!	Sommer2026!

Solche Muster sind leicht erkennbar. Angriffsprogramme passen gezielt einzelne Teile an. Sie ändern Jahreszahlen, ersetzen Zeichen oder variieren Gross und Kleinschreibung. Dadurch bleiben auch leicht abgeänderte Passwörter angreifbar.

Typische Fehler bei Passwörtern erstellen und warum sie unsicher sind:

123456, 123456789
Einfache Zahlenfolgen stehen ganz oben in Angriffslisten

Passwort, Passwort123!, Sommer2026!
Häufige Wörter wie „Passwort“ oder „Sommer“ sind in Wörterbüchern enthalten

Anna1952
Namen von Kindern oder Partnern sind oft öffentlich sichtbar

Bello2010!
Haustiernamen werden häufig geteilt oder sind bekannt

SaraGeburtstag
Geburtsdaten finden sich in Profilen oder Dokumenten

St@dt2024!, C0mputer-0102
Ersetzungen wie a zu @ oder o zu 0 sind bekannt und werden automatisch getestet

Angriffsprogramme arbeiten systematisch. Sie kombinieren Wörter, Namen und Zahlen aus grossen Datenbanken und testen diese automatisiert gegen viele Dienste gleichzeitig.

Klare Regel

- Jedes Konto erhält ein eigenes Passwort
- Keine Wiederverwendung
- Keine erkennbaren Muster
- Keine persönlichen Informationen

Setze das konsequent um. Ein einzelnes schwaches Passwort reicht aus, um mehrere Konten zu gefährden.

Wie erstellt man ein sicheres Passwort

Es wird empfohlen, lange, einzigartige und nicht erratbare Passwörter zu verwenden. Nimm drei Teile, die du dir gut merkst, die andere aber nicht erraten. Verwende Wörter, die für dich persönlich merkbar sind und nicht online mit dir in Verbindung stehen. Besonders soziale Medien sind ein Ort, an dem man oft unbewusst viele persönliche Informationen preisgibt.

Eine einfache Methode hilft dir dabei

Teil 1:
Ein alter Ort oder ein Erinnerungswort, zum Beispiel die Strasse, in der du als Kind gelebt hast, oder ein Ort, an dem deine Grosseltern gelebt haben.

Beispiel: Kornweg

Teil 2:
Eine Zahl, die kein Geburtsdatum ist, zum Beispiel deine Lieblingszahl, oder eine Zahl aus der Strecke deines Lieblingsflusses. Wichtig ist, dass dir die Zahl später leicht in den Sinn kommt, wenn du das Passwort verwendest.
Beispiel: 7432

Teil 3:
Ein fremdsprachiges Wort kann helfen, wenn es selten ist oder ungewöhnlich kombiniert wird. Es erhöht die Vielfalt, aber der Hauptschutz kommt von der Länge und der Kombination mehrerer Teile.

Beispiel: Papillon

Sonderzeichen

Setze Sonderzeichen zwischen die Teile, nicht immer ans Ende. So entsteht kein typisches Muster. Ein Wort, eine Jahreszahl und ein Ausrufezeichen sind ein bekanntes Muster. Solche Kombinationen stehen in vielen Angriffslisten und werden gezielt getestet.

Ergebnis:

Kornweg!7432Papillon

Warum ist das gut?

20 Zeichen, Gross und Kleinbuchstaben, Zahlen, Sonderzeichen, persönlich merkbar und nicht direkt aus Familie, Haustier oder Geburtstag ableitbar

Ein gutes Passwort muss nicht wie Zeichensalat aussehen. Eine kleine private Geschichte hilft beim Merken.

So bleibt es merkbar

- Nutze ein Bild aus deiner Erinnerung
- Verwende keine Namen aus deiner Familie
- Verwende kein Geburtsdatum
- Verwende keinen aktuellen Wohnort
- Nutze ein fremdsprachiges Wort, das du kennst
- Halte die Reihenfolge immer gleich

Weitere gute Muster:

Rigi!7432Tulipe, Tasse?6294Lisbona, Garten!3817Nube, Tee?um9InPorto

Was würdest du bei einem langen Passwort immer noch falsch machen?

Nehmen wir das Beispiel «Kornweg!7432Papillon». Im Vergleich dazu sind «Kornweg!8005Zürich» oder «Kornweg!7432nonna» schwächer.

Bei «Kornweg!7432Papillon» haben die Teile keinen offensichtlichen Zusammenhang. Die Wörter stammen aus unterschiedlichen Kontexten, die Zahl ist zufällig. Das erschwert das Erraten.

Bei «Kornweg!8005Zürich» besteht ein klarer Bezug. Kornweg ist eine Strasse, 8005 ist eine reale Postleitzahl in Zürich, und Zürich ist der Ort dazu. Diese Kombination ist logisch verknüpft und damit vorhersehbarer.

Auch «Kornweg!7432nonna» ist schwächer, wenn «nonna» einen persönlichen Bezug hat. Solche Begriffe lassen sich oft aus sozialen Informationen ableiten.

Wichtig ist: Auch ein langes Passwort bleibt unsicher, wenn die Bestandteile logisch zusammenhängen oder persönliche Bezüge haben.

Fazit:

- Keine erkennbaren Zusammenhänge zwischen den Teilen
- Keine realen Kombinationen wie Ort und Postleitzahl
- Keine persönlichen Begriffe aus deinem Umfeld
- Zufällige oder unabhängige Elemente kombinieren

So bleibt auch ein langes Passwort schwer erratbar.

Nimm dieses Beispiel nicht als echtes Passwort. Es steht jetzt öffentlich in dieser Anleitung.

Zusätzliche Tipps und Tricks

Für viele Konten ist ein Passwortmanager sinnvoll. Er speichert Passwörter verschlüsselt und benötigt ein starkes Masterpasswort. Das National Institute of Standards and Technology und das Nationales Zentrum für Cybersicherheit empfehlen den Einsatz solcher Lösungen.

Falls du ein Passwort aufschreibst:

- Lege es in einen verschlossenen Umschlag
- Bewahre den Umschlag in einer abschliessbaren Schublade auf
- Schreibe keinen Hinweis wie «Bank Passwort» darauf
- Klebe es nicht an Bildschirm, Tastatur oder Telefon
- Speichere es nicht ungeschützt im Handy

Diese Regeln reduzieren das Risiko, dass Passwörter entdeckt oder missbraucht werden.