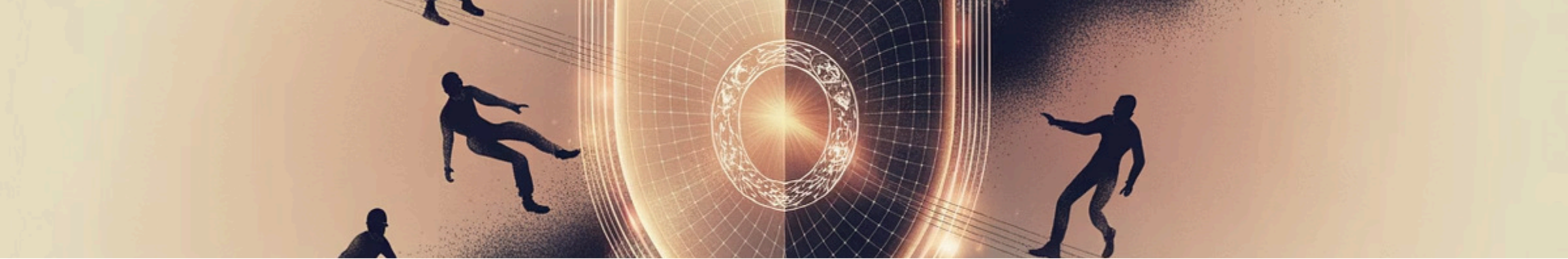




## **Sicher authentifizieren: Passwörter, 2FA & Passkeys einfach erklärt**

In unserer zunehmend digitalisierten Welt ist sichere Authentifizierung wichtiger denn je. Von einfachen Passwörtern über Zwei-Faktor-Authentifizierung bis hin zu innovativen Passkeys - entdecken Sie, wie sich die digitale Sicherheit entwickelt und welche Lösungen heute den besten Schutz bieten.



# Warum brauchen wir Authentifizierung?

Authentifizierung ist das digitale Äquivalent zur Identitätsprüfung in der physischen Welt. Während wir in der realen Welt unseren Personalausweis vorzeigen, müssen wir online beweisen, dass wir berechtigt sind, auf bestimmte Daten und Dienste zuzugreifen.

Die Bedrohungslage ist alarmierend: Cyberkriminelle werden immer raffinierter und nutzen ausgeklügelte Methoden, um an sensible Informationen zu gelangen. Ohne wirksame Authentifizierung stehen Millionen von persönlichen und geschäftlichen Daten schutzlos da.

## 81%

**Datenlecks durch Passwörter**

Aller Sicherheitsvorfälle 2024 entstanden durch gestohlene oder schwache Passwörter (Verizon DBIR)

## 24Mrd

**Angriffe pro Jahr**

Weltweite Cyber-Attacken mit steigender Tendenz

# Passwörter: Das klassische Schutzschild

Passwörter sind seit Jahrzehnten die Grundlage der digitalen Sicherheit. Das Konzept ist einfach: Nutzer erstellen eine geheime Zeichenkombination, die nur sie kennen, um ihre Identität zu beweisen. Diese "geteilten Geheimnisse" werden sowohl beim Nutzer als auch beim Dienst gespeichert und bei jeder Anmeldung abgeglichen.

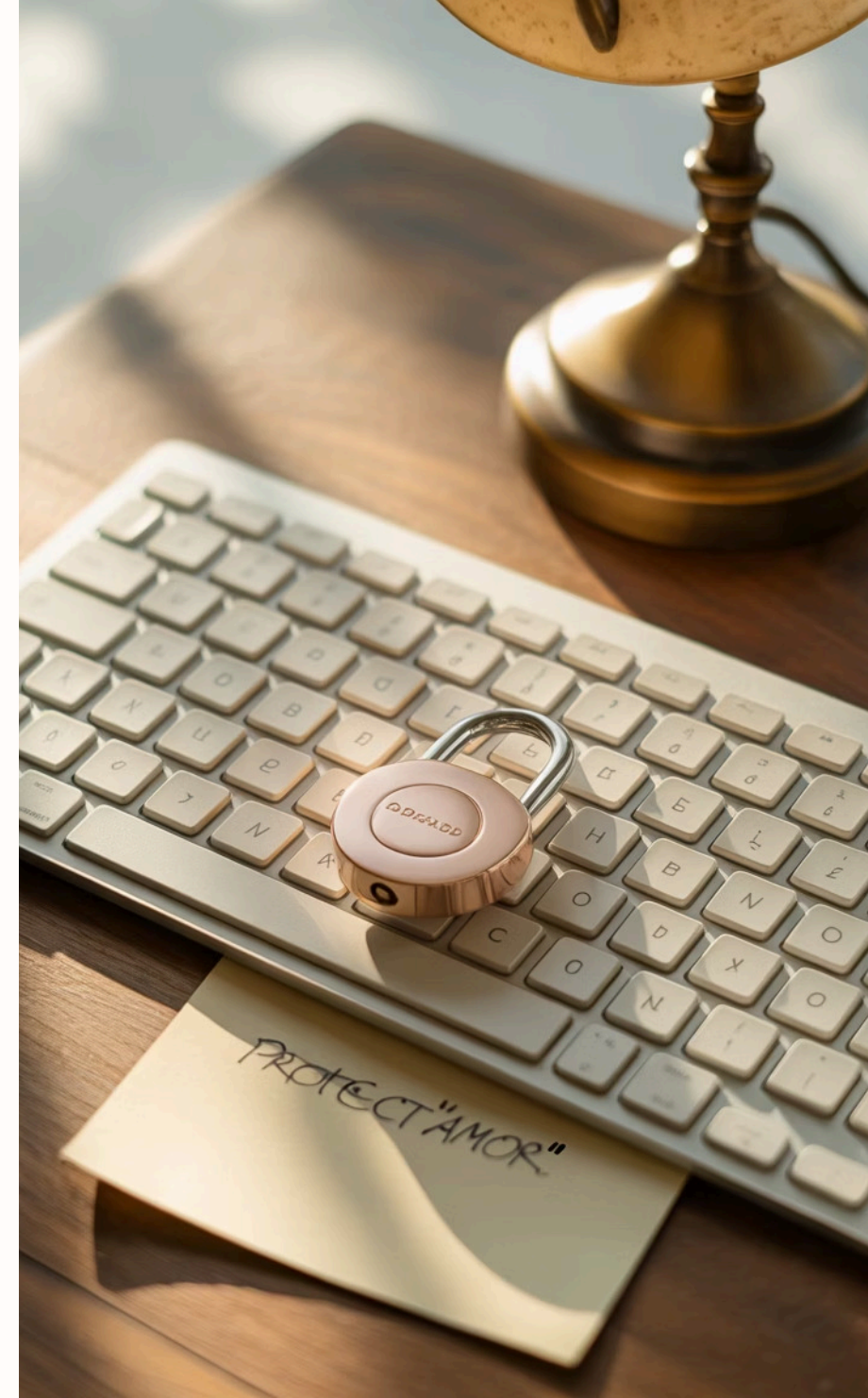
## Wie Passwörter funktionieren

Der Nutzer gibt seine gewählte Zeichenkombination ein, die mit der gespeicherten Version verglichen wird. Bei Übereinstimmung wird der Zugang gewährt.

## Die größten Schwachstellen

Wiederverwendung identischer Passwörter, zu einfache Kombinationen, Phishing-Angriffe und Datenlecks bei Anbietern gefährden die Sicherheit.

⊗ **Alarmierende Statistik:** 2023 wurden 60% aller kompromittierten Konten durch Passwortdiebstahl angegriffen. Die durchschnittliche Person verwendet dasselbe Passwort für 14 verschiedene Accounts.



# Zwei-Faktor-Authentifizierung (2FA): Mehr Sicherheit durch zweite Ebene

Die Zwei-Faktor-Authentifizierung revolutioniert die Sicherheit, indem sie das Prinzip "etwas, was Sie wissen" (Passwort) mit "etwas, was Sie haben" (Gerät) oder "etwas, was Sie sind" (Biometrie) kombiniert. Selbst wenn Cyberkriminelle Ihr Passwort stehlen, benötigen sie zusätzlich Zugang zu Ihrem zweiten Faktor.

01

## SMS-basierte Codes

Einmalcodes werden per Textnachricht an Ihr registriertes Handy gesendet. Schnell verfügbar, aber anfällig für SIM-Swapping-Angriffe.

02

## Authenticator-Apps (TOTP)

Apps wie Google Authenticator generieren zeitbasierte Codes offline auf Ihrem Gerät. Sicherer als SMS, funktioniert auch ohne Internetverbindung.

03

## Hardware-Token

Physische Geräte wie YubiKeys bieten höchste Sicherheit durch kryptographische Schlüssel, die nicht kopiert werden können.

## Vorteile von 2FA

- Drastische Reduzierung erfolgreicher Angriffe (um bis zu 99,9%)
- Schutz auch bei Passwort-Kompromittierung
- Compliance mit Sicherheitsstandards

## Nachteile und Herausforderungen

- SMS-Codes können abgefangen werden
- Zusätzlicher Zeitaufwand bei jeder Anmeldung
- Potenzielle Nutzerfrustration und Abbruchrate

# 2FA: Der doppelte Schutz

Die Kombination aus Wissen und Besitz macht Ihre Konten deutlich sicherer. Moderne 2FA-Methoden bieten verschiedene Sicherheitsstufen für unterschiedliche Anforderungen.



# Passkeys: Die Zukunft der Authentifizierung

Passkeys markieren einen Paradigmenwechsel in der digitalen Authentifizierung. Statt auf geteilte Geheimnisse zu setzen, nutzen sie asymmetrische Kryptographie nach dem FIDO2-Standard. Das Ergebnis: passwortloses Anmelden mit maximaler Sicherheit.

1

## **Biometrische Geräteentsperrung**

Fingerabdruck, Face ID, Windows Hello oder einfache Geräte-PIN ersetzen komplizierte Passwörter komplett.

2

## **Public-Key-Kryptographie**

Ein Schlüsselpaar wird generiert: Der private Schlüssel bleibt sicher auf Ihrem Gerät, der öffentliche wird beim Dienst hinterlegt.

3

## **Phishing-Immunität**

Da keine Passwörter übertragen werden, sind Phishing-Angriffe und Credential-Stuffing unmöglich.

- ✔ **Technischer Durchbruch:** Passkeys kombinieren die Sicherheit von Hardware-Token mit der Benutzerfreundlichkeit von biometrischen Systemen - ohne die Nachteile traditioneller Methoden.



# Passkeys vs. 2FA: Was macht Passkeys besser?

## Traditionelle 2FA

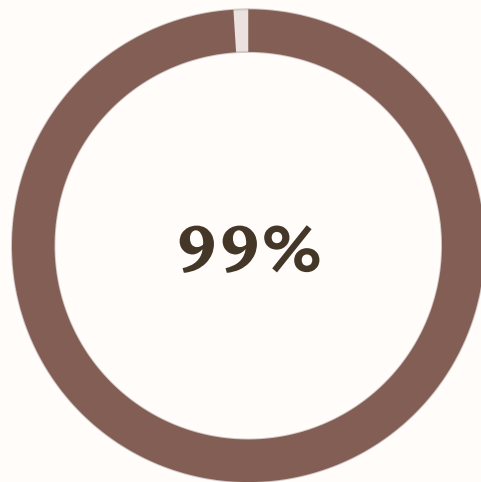
Zwei-Faktor-Authentifizierung ergänzt bestehende Passwörter um eine zusätzliche Sicherheitsebene. Trotz deutlich verbesserter Sicherheit bleiben fundamentale Schwächen:

- Passwörter bleiben weiterhin angreifbar
- SMS-Codes können durch SIM-Swapping kompromittiert werden
- Mehrere Schritte verlängern den Anmeldeprozess
- Nutzer können 2FA-Codes verlieren oder vergessen

## Moderne Passkeys

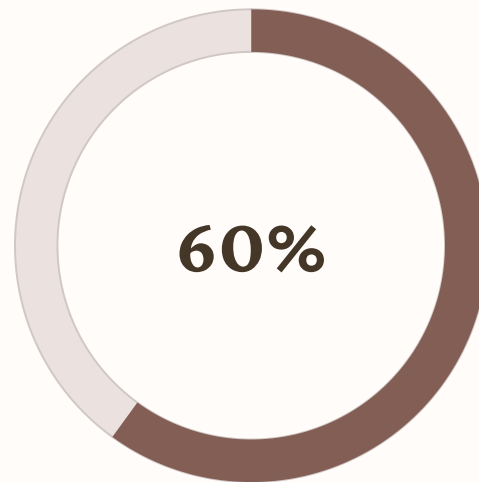
Passkeys revolutionieren die Authentifizierung durch vollständigen Ersatz traditioneller Passwörter mit kryptographischen Schlüsseln:

- Komplette Eliminierung von Passwörtern und deren Schwächen
- Kein Übertragungsweg für Angreifer vorhanden
- Multi-Faktor-Sicherheit in einem einzigen, nahtlosen Schritt
- 20% höhere Anmeldeerfolgsrate durch intuitive Bedienung



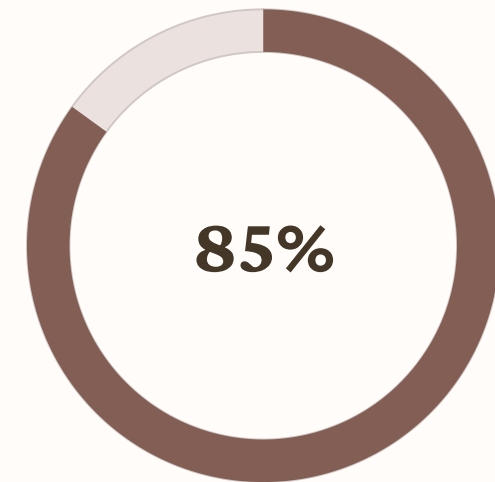
### Phishing-Schutz

Passkeys sind praktisch immun gegen alle Phishing-Versuche



### Zeitersparnis

Schnellere Anmeldung im Vergleich zu traditioneller 2FA



### Nutzerakzeptanz

Höhere Zufriedenheit bei Passkey-Nutzern

# Wie ein Passkey funktioniert: Schritt für Schritt

Passkeys nutzen ein hochmodernes kryptografisches Verfahren, um eine sichere, passwortlose Anmeldung zu ermöglichen. Es basiert auf Public-Key-Kryptographie, die traditionelle Passwörter überflüssig macht.



## Schlüsselpaar-Erzeugung

Bei der Registrierung generiert Ihr Gerät ein einzigartiges kryptografisches Schlüsselpaar: einen privaten und einen öffentlichen Schlüssel.



## Sichere Speicherung

Der private Schlüssel bleibt sicher und verschlüsselt auf Ihrem Gerät. Der öffentliche Schlüssel wird sicher beim Dienstanbieter hinterlegt.



## Anmeldung per Biometrie/PIN

Bei der Anmeldung wird der private Schlüssel durch Ihre Biometrie (Fingerabdruck, Face ID) oder PIN freigeschaltet und signiert eine Challenge des Servers.



## Verifizierung des Servers

Der Dienstanbieter überprüft die Signatur mit Ihrem öffentlichen Schlüssel. Wenn sie übereinstimmt, wird der Zugriff sofort gewährt.

# Geräteverlust: Passkeys sicher wiederherstellen

Eines der Hauptanliegen beim Übergang zu Passkeys ist die Frage, was passiert, wenn das Gerät, auf dem sie gespeichert sind, verloren geht. Passkeys sind so konzipiert, dass sie sicher und flexibel über mehrere Geräte hinweg verfügbar und wiederherstellbar sind.

## Cloud-Synchronisierung

Passkeys werden verschlüsselt und sicher über Cloud-Dienste wie Apples iCloud Schlüsselbund oder den Google Password Manager auf all Ihre vertrauenswürdigen Geräte synchronisiert. Geht ein Gerät verloren, sind Ihre Passkeys auf den anderen Geräten weiterhin zugänglich.

## Einfache Übertragung

Beim Einrichten eines neuen Geräts können Sie Ihre Passkeys in der Regel mit wenigen Schritten aus der Cloud wiederherstellen. Alternativ lassen sich Passkeys oft auch direkt von einem bestehenden Gerät auf ein neues übertragen, beispielsweise via QR-Code.

## Notfall-Wiederherstellung

Sollten Sie alle Ihre Geräte verlieren, bieten die Anbieter der Cloud-Dienste robuste Mechanismen zur Kontowiederherstellung. Dies ermöglicht es Ihnen, den Zugang zu Ihrem Cloud-Konto und somit zu Ihren Passkeys sicher wiederherzustellen, ohne Ihr Passwort zu benötigen.

- ☐ **Passkeys sind geräteübergreifend:** Im Gegensatz zu traditionellen Passwörtern, die an ein einzelnes Konto gebunden sind, sind Passkeys für eine einfache Nutzung über all Ihre Geräte hinweg konzipiert und bieten dennoch höchste Sicherheit.

# Vorbereitung ist alles: Was tun vor dem Geräteverlust?

Auch wenn Passkeys auf maximale Sicherheit und einfache Wiederherstellung ausgelegt sind, gibt es proaktive Schritte, die Sie unternehmen können, um im Ernstfall bestens vorbereitet zu sein und einen nahtlosen Übergang zu gewährleisten.



## Cloud-Synchronisierung sicherstellen

Aktivieren und überprüfen Sie die automatische Synchronisierung Ihrer Passkeys über vertrauenswürdige Cloud-Dienste (z.B. iCloud Schlüsselbund, Google Password Manager). Dies hält Ihre Passkeys aktuell und über alle Ihre Geräte verteilt.



## Passkeys auf mehreren Geräten einrichten

Hinterlegen Sie Passkeys für wichtige Konten nicht nur auf einem, sondern auf mindestens zwei Ihrer vertrauenswürdigen Geräte (z.B. Smartphone und Laptop). So haben Sie immer eine Ausweichmöglichkeit, falls ein Gerät ausfällt.



## Wiederherstellungsmethoden prüfen

Machen Sie sich mit den spezifischen Wiederherstellungsoptionen Ihres Cloud-Dienstes vertraut. Informieren Sie sich, welche Schritte im Falle eines vollständigen Geräteverlusts nötig sind, um Ihr Konto und damit Ihre Passkeys wiederherzustellen.



# Sicherer, schneller, einfacher

Der Vergleich zeigt deutlich: Während traditionelle Authentifizierung mehrere komplexe Schritte erfordert, vereinfachen Passkeys den Prozess auf eine einzige, sichere Aktion.

# Fazit: Auf dem Weg zur passwortlosen Zukunft

## 1 Heute: Passwort-Dominanz

Passwörter bleiben Standard, aber ihre Schwächen werden täglich deutlicher. Millionen von Nutzern kämpfen mit unsicheren, schwer zu merkenden Kombinationen.

## 3 Zukunft: Passkey-Revolution

Passkeys vereinen höchste Sicherheit mit maximaler Benutzerfreundlichkeit und sind immun gegen moderne Cyber-Bedrohungen.

1

2

3

## Übergangsphase: 2FA als Brücke

Zwei-Faktor-Authentifizierung bietet deutlich mehr Sicherheit, bringt aber zusätzliche Komplexität für Nutzer und bleibt anfällig für bestimmte Angriffe.

## Unsere Empfehlung

Nutzen Sie Passkeys überall dort, wo sie verfügbar sind. Die Technologie bietet nicht nur besseren Schutz, sondern auch ein deutlich angenehmeres Nutzererlebnis.

Für Bereiche ohne Passkey-Unterstützung aktivieren Sie mindestens 2FA - jede zusätzliche Sicherheitsebene zählt.

✔ **Der Wandel hat begonnen:** Mit der wachsenden Akzeptanz von Passkeys stehen wir am Beginn einer neuen Ära der digitalen Sicherheit - einfacher, sicherer und nutzerfreundlicher als je zuvor.