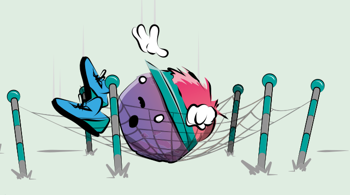
Wumbel®

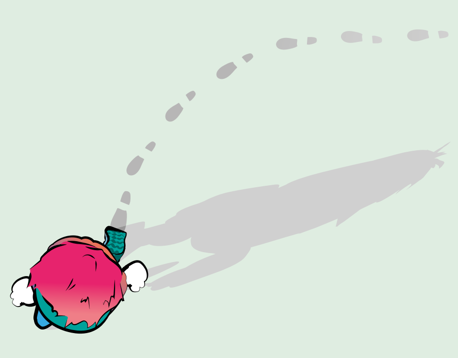
Die Notwendigkeit von 2FA

SCON

Die Notwendigkeit der Zwei-Faktor-Authentifizierung im digitalen Zeitalter

Ob beim bequemen Online-Shopping, dem Austausch in sozialen Netzwerken oder der Verwaltung wichtiger Finanzdaten, wir hinterlegen **kontinuierlich sensible Informationen** im digitalen Raum. Diese Fülle an persönlichen Daten macht uns jedoch auch zu **attraktiven Zielen** für Cyberkriminelle, deren Methoden immer ausgefeilter und schwerer zu durchschauen werden. Während Passwörter nach wie vor **die erste Verteidigungslinie** für unsere digitalen Identitäten darstellen, bieten sie **allein längst keinen ausreichenden Schutz** mehr. Hier kommt die **Zwei-Faktor-Authentifizierung (2FA)** ins Spiel: Ein robuster Schutzmechanismus, der eine **zweite Sicherheitsebene** schafft und Ihre Konten effektiv absichert selbst dann, **wenn Ihr primäres Passwort kompromittiert wurde.**





Warum ist die Zwei-Faktor-Authentifizierung so entscheidend?

Die Zwei-Faktor-Authentifizierung (2FA) bietet hier eine **signifikante Verbesserung** der Sicherheit, indem sie eine zweite, **unabhängige** Bestätigung Ihrer Identität für den Login-Prozess erfordert. Diese zusätzliche Hürde basiert auf unterschiedlichen Kategorien von Faktoren:

Beispiele für zweite Faktoren: **Einmal-Code per SMS/App** oder **E-Mail, biometrische Daten, physischer Schlüssel.**

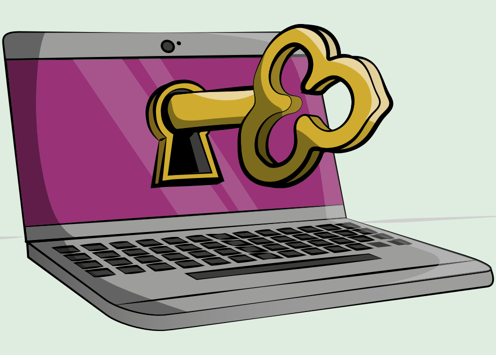
Passwörter sind anfällig für **Phishing, Datenlecks** und **Brute-Force-Attacken*.**

2FA **erfordert eine zweite Bestätigung** beim Login. Ohne den zweiten Faktor ist der Zugriff trotz bekanntem Passwort **unmöglich.**

Selbst wenn es einem Angreifer gelingen sollte, Ihr Passwort zu **entwenden oder zu erraten**, fehlt ihm ohne den zweiten, unabhängigen Faktor der Zugriff auf Ihr Konto. Diese **zusätzliche Barriere** macht es für unbefugte Dritte **erheblich schwerer**, sich Zugang zu Ihren sensiblen Informationen zu verschaffen.

Passkeys: Die nächste Generation der sicheren Anmeldung

Als Weiterentwicklung im Bereich der Authentifizierung etablieren sich zunehmend **Passkeys.** Diese innovative Technologie **ersetzt herkömmliche, oft unsichere Passwörter** durch eindeutige, **kryptografische Schlüssel**, die sicher auf Ihren persönlichen Geräten (z. B. Smartphone, Laptop) gespeichert werden. Dies birgt mehrere **wesentliche Vorteile:**

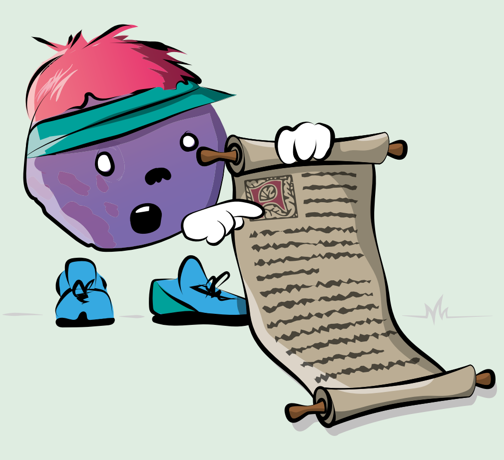


Abschied von Passwörtern:
Sie müssen sich keine komplexen und unterschiedlichen Passwörter **mehr merken.**

Effektiver Schutz vor Phishing:
Da Passkeys fest an Ihre **Geräte gebunden** sind und auf kryptografischen Signaturen basieren, können sie von Angreifern **nicht so einfach gestohlen** oder durch **Phishing-Websites abgefangen werden.**

Intuitive Bedienung:
Das Einloggen erfolgt in der Regel **nahtlos über die vertrauenswürdige Benutzerverifizierung** per biometrischer Authentifizierung **(Fingerabdruck oder Gesichtserkennung)** oder seltener durch eine Geräte-PIN.

Der feine Unterschied: Zwei-Faktor-Authentifizierung (2FA) VS Multifaktor-Authentifizierung (MFA)

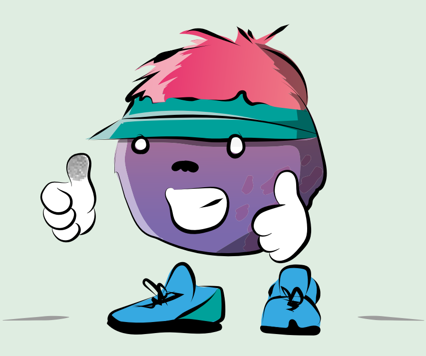


1.) Ein Passwort oder ein moderner Passkey als **primäre Authentifizierung.**

2.) Ein **zeitgebundener Einmal-Code** aus einer dedizierten Authenticator-App als **zweite Ebene.**

3.) Eine **abschließende biometrische Verifizierung** mittels Gesichtserkennung oder Fingerabdruck als **dritte Sicherheitsstufe.**

Dieser **mehrschichtige Ansatz macht es Cyberkriminellen schwer,** die verschiedenen Schutzmechanismen **gleichzeitig zu überwinden** und sich unbefugten Zugriff zu verschaffen.



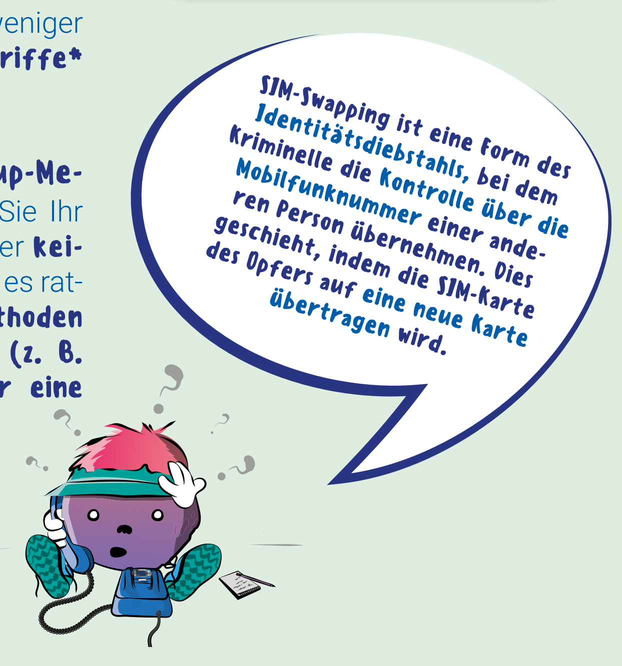
So aktivieren Sie die Zwei-Faktor-Authentifizierung

1.) Überprüfen Sie Ihre Kontoeinstellungen: Nahezu alle gängigen Online-Dienste und Plattformen (wie Google, Apple, Facebook, Ihre Bank etc.) bieten die 2FA als zusätzliche Sicherheitsoption in ihren Einstellungen an. Suchen Sie nach Begriffen wie **"Sicherheit", "Anmeldung"** oder **"Zwei-Faktor-Authentifizierung".**

2.) Wählen Sie eine sichere Methode: Obwohl die SMS-basierte 2FA eine einfache Einstiegsmöglichkeit bietet, gelten Authenticator-Apps wie **Google Authenticator** oder **Microsoft Authenticator** als sicherer, da sie **Einmal-Codes offline generieren** und somit weniger anfällig für **SIM-Swapping-Angriffe*** sind.

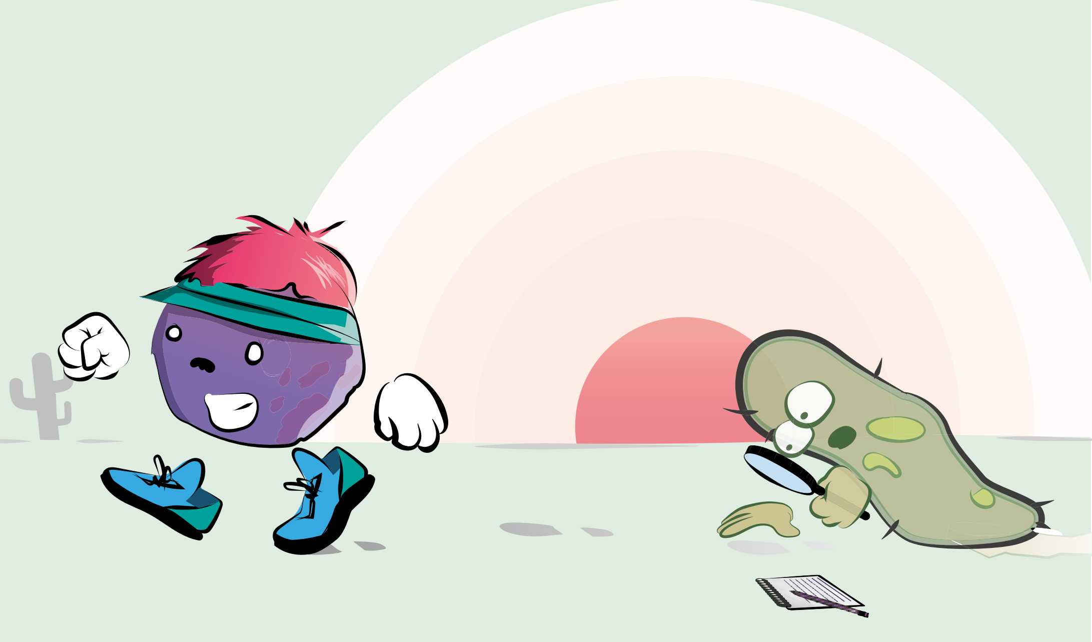
3.) Hinterlegen Sie Backup-Methoden: Für den Fall, dass Sie Ihr primäres Gerät **verlieren** oder **keinen Zugriff** darauf haben, ist es ratsam, **alternative Zugriffsmethoden** für die 2FA zu konfigurieren **(z. B. Wiederherstellungscodes oder eine alternative Telefonnummer).**

Die Nutzung der Zwei-Faktor-Authentifizierung ist in der Regel **unkompliziert** und sollte für **jeden Nutzer zur Standardpraxis** werden:



Standardmäßige Installation der Authenticator-App bei der Geräteeinrichtung

Bei der Einrichtung neuer Diensthandys sollte eine sichere **Authenticator App vorinstalliert** sein und die **Aktivierung der 2FA verpflichtend** sein. Dies gewährleistet die sofortige Nutzung der Zwei-Fator-Authentifizierung durch alle Mitarbeiter und **schützt geschäftliche Online-Konten** optimal vor unbefugtem Zugriff. Angesichts zunehmender Cyberangriffe ist **diese grundlegende Sicherheitsmaßnahme** bei der Gerätekonfiguration unerlässlich für eine **konsequente Umsetzung wichtiger Sicherheitsrichtlinien** von Anfang an.



Fazit:
Ihre digitale Sicherheit liegt in Ihren Händen!

Die Bedrohung durch Cyberkriminalität **nimmt kontinuierlich zu,** doch Sie haben die Möglichkeit dieser Entwicklung **entgegenzuwirken.** Mit den richtigen Vorsichtsmaßnahmen können Online-Konten effektiv geschützet werden. Die **Zwei-Faktor-Authentifizierung** & **moderne Passkeys** und die **umfassendere Multifaktor-Authentifizierung stellen einfache**, aber äußerst wirkungsvolle Maßnahmen dar, um Ihre wertvollen und sensiblen Daten vor den Zugriffen von Hackern **zu bewahren.**

Wumbel®

S-CON GmbH & Co. KG
Podbielskistraße 386
30659 Hannover
Servicenummer: 0800 88446688
E-Mail: office@s-con.de

SCON