2FA

Zwei-Faktor-Authentifizierung

(auch MFA = Multi-Faktor-Authentifizierung)

café digital

▶2FA – Zwei-Faktor-Authentifizierung

Authentifizierung

Wenn man sich auf einer Webseite oder bei einer App mit seinem **Benutzernamen** und **Passwort** anmeldet, wird geprüft, ob die Eingabe korrekt ist.

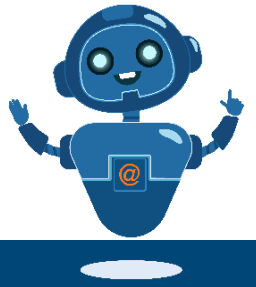
Wenn Webseite oder App melden, dass die Eingabe korrekt ist, wird die Anmeldung durchgeführt.

Die Prüfung der Kombination von Benutzername + Passwort, nennt man **Authentifizierung**.

Die Anmeldung mit der Kombination von Benutzername + Passwort ist sicher, sofern man ein starkes Passwort benutzt.

Normalerweise reicht **1 Faktor**, nämlich die (korrekte) Kombination von **Benutzername + Passwort** für die Anmeldung.

Sicherer wird es, wenn ein **2. Faktor** für die für die erfolgreiche Anmeldung notwendig ist!



▶2FA - Zwei-Faktor-Authentifizierung

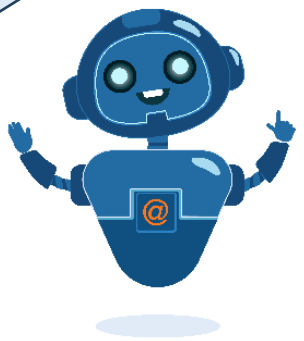
Warum ein 2. Faktor?

Wenn man ein Benutzerkonto **besonders schützen** möchte, kann man inzwischen auf vielen Webseiten einen **2. Faktor** bei der Anmeldung **hinzufügen**.

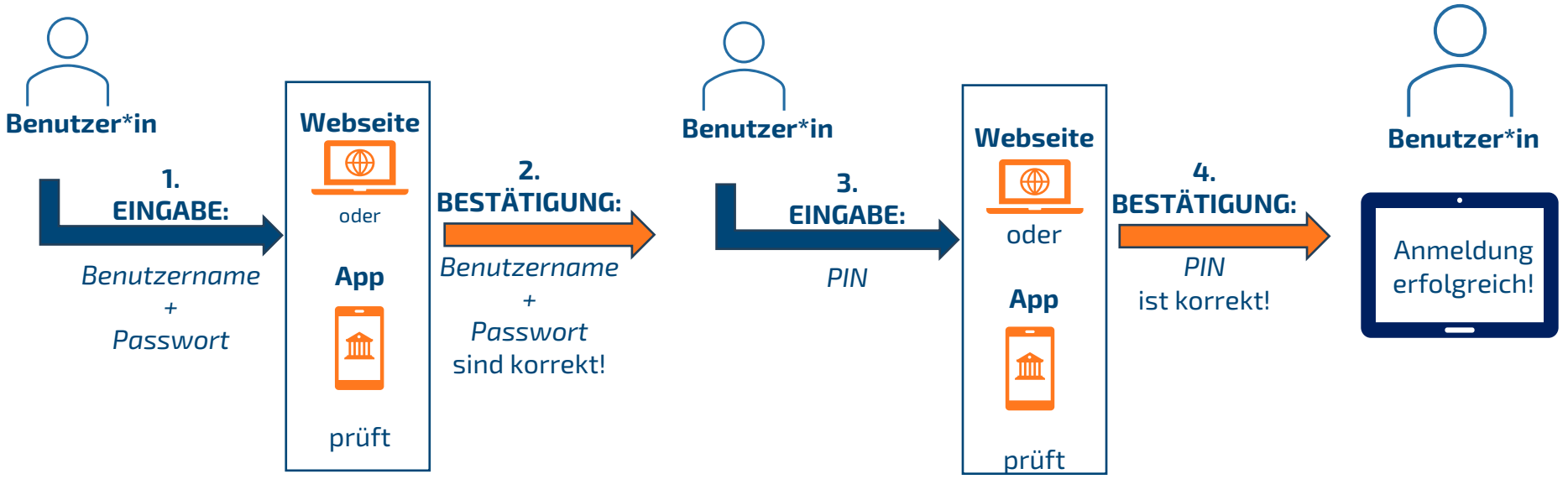
Das ist meist ein Zahlen- oder Buchstabencode (**PIN**), den man **per E-Mail oder SMS** erhält oder über eine **Authentifizierungs-App** (auf dem Handy) abruft und in einem 2. Schritt bei der Anmeldung eingeben muss.

Benutzername + Passwort (1. Faktor)
+ PIN (2. Faktor)
=
2 Faktoren für Authentifizierung

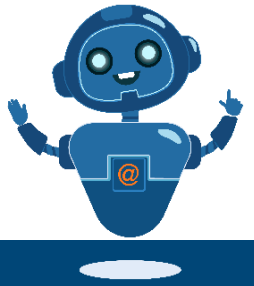
Statt **2FA/Zwei-Faktor-Authentifizierung**, wird die Anmeldung mit mehr als einem Faktor manchmal auch als **MFA/Mehr-Faktor-Authentifizierung** bezeichnet.



▶2FA – Zwei-Faktor-Authentifizierung



Mit 2FA dauert die Anmeldung zwar etwas länger, dafür ist das Benutzerkonto aber auch **DOPPELT** geschützt!



café digital

▶2FA - Zwei-Faktor-Authentifizierung

Warum ist eine PIN nur kurze Zeit gültig?

PINs, die in einer Authentifizierungs-App angezeigt werden, sind nur 30 Sekunden lang gültig. PINs, die per E-Mail oder SMS verschickt werden, können auch mehrere Minuten (selten auch Stunden) gültig sein.

Die **kurze Gültigkeitsdauer** von PINs ist ein **Sicherheitsfaktor**, der den Zugang zu einem Benutzerkonto durch fremde Personen verhindern soll.

Wie? Die PIN wird nur an ***Ihre* E-Mailadresse** oder **auf *Ihr* Handy per SMS** geschickt oder die Authentifizierungs-App, die **auf *Ihrem* Handy installiert** ist, zeigt die PIN an. So können auch **nur *Sie*** innerhalb der Gültigkeitsdauer die PIN eingeben.

Selbst wenn also ein Fremder Ihren Benutzernamen + Passwort herausfinden würde, könnte diese Person sich an einem mit 2FA geschützten Benutzerkonto **NICHT** anmelden, da nur ***SIE*** Zugang zur PIN haben.

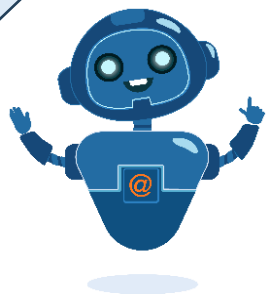
Was ist TOTP?

TOTP ist nur eine andere Bezeichnung für die Zwei-Faktor-Authentifizierung.

TOTP ist die Abkürzung für:

Time-based	zeit-basiertes
One-**T**ime	einmaliges
Password	Passwort

Das zeit-basierte einmalige Passwort ist die **PIN,** von der in diesem Learning-Nugget die Rede ist.



café digital