

## Wie richtet man die zweistufige Authentifizierung ein?

Die Einrichtung der 2FA variiert von Plattform zu Plattform, aber im Allgemeinen sind die Schritte recht ähnlich:

- 1. Gehen Sie in die Sicherheitseinstellungen** des Accounts, den Sie absichern möchten.
- 2. Suchen Sie** nach der Option um 2FA zu aktivieren, und wählen Sie sie aus.
- 3. Wählen Sie den zweiten Faktor**, den Sie verwenden möchten (z. B. SMS, Authentifizierungs-App usw.).
- 4. Folgen Sie den Anweisungen auf dem Bildschirm**, um den zweiten Faktor zu konfigurieren.
- 5. Testen Sie**, ob alles richtig eingestellt ist, indem Sie sich abmelden und mit dem zweiten Faktor erneut anmelden.



Safeonweb<sup>.be</sup>

## Womit soll ich anfangen?

- Fangen Sie mit Ihrem E-Mail Account an.
- Aktivieren Sie 2FA dann auf den Internetseiten auf denen Sie Ihre Bankdaten hinterlegt haben: Webshops, Buchungswebsites, Ticketverkäufer, usw.
- Ihre sozialen Netzwerke.

**Machen Sie es sich zur Gewohnheit, 2FA überall zu benutzen, wo es möglich ist.**

## Brauchen Sie Hilfe?

Zögern Sie nicht, Ihre Familie oder Freunde um Hilfe zu bitten. Sie können Ihre Fragen auch in einem der vielen EPN (Espaces publics numériques) in der Wallonie und Brüssel, bzw. Digipoints in Flandern stellen.



**Möchten Sie mehr über zweistufige Authentifizierung erfahren?**

Surfen Sie auf [safeonweb.be](https://safeonweb.be)

# Machen Sie es wie Herstappe: Halten Sie Cyber-Kriminelle fern



Schützen Sie Ihre Online-Accounts mit der zweistufigen Authentifizierung.  
Surfen Sie schnell auf [safeonweb.be](https://safeonweb.be)



Safeonweb.be

Wenn ein Hacker oder  
Betrüger Ihr Passwort  
in die Hände bekommt,  
kann er



**Ihre Mailbox  
benutzen**



**an Ihrer Stelle auf Ihrem  
Konto Videospiele spielen**



**Bestellungen in Ihrem  
Namen aufgeben**



**etwas auf Facebook  
posten, usw.**

## Wie kommen Betrüger an meine Passwörter?

Die Verwendung von starken Passwörtern ist notwendig, aber dies alleine schützt Sie nicht ausreichend. Passwörter werden von Betrügern gestohlen oder erraten. Oder aber stehlen Betrüger ihre Passwörter durch diese Tricks (sie fragen am Telefon unter einem Vorwand danach oder bringen Sie dazu, sie auf einer gefälschten Website einzugeben). Die Wahrscheinlichkeit, dass eines Ihrer Passwörter gerade jetzt im Internet zu sehen ist, ist ziemlich hoch.

## Zweistufige was?

Die gute Nachricht ist, dass Sie so etwas vermeiden können, indem Sie, wann und wo immer möglich, zusätzlich zu Ihrem Passwort einen zweiten Schlüssel verwenden: z. B. Gesichtserkennung oder einen Fingerabdruck, oder einen an Ihr Mobiltelefon gesendeten Code. Ein Betrüger kann zwar an Ihr Passwort kommen, doch ohne den zweiten Schlüssel ist es wertlos. Dies nennt man zweistufige Authentifizierung, oder "2FA". Im Grunde kennen Sie das schon: itsme ist eine Form der 2FA, und der Digipas beim Online-Banking ist ebenfalls ein zweiter Schlüssel.



**Safeonweb**<sup>be</sup>

Um Zugang zu Ihrem Account zu erhalten, müssen Sie beweisen, dass Sie derjenige sind, der Sie vorgeben zu sein.

Dies kann auf drei Arten bzw. mit drei Faktoren geschehen:

1. mit **etwas, das nur Sie kennen** (Ihr Passwort oder Ihren PIN),



2. mit **etwas, das nur Sie haben** (ein Code, den Sie auf Ihrem Telefon oder in Ihrer Authentifizierungs-App erhalten),



3. mit **etwas, das nur Sie sind** (Ihr Fingerabdruck, Ihr Gesicht, Ihre Iris,...).



Normalerweise verwenden Sie einen dieser Faktoren, oft ein Passwort, um zu beweisen, wer Sie sind. Aber es ist besser, zwei oder mehr Faktoren zu verwenden: Das ist die zwei- oder mehrstufige Authentifizierung (2FA oder MFA). Sie verwenden dann z. B. ein Passwort und einen zusätzlichen Code, der an Ihr Mobiltelefon gesendet wird, oder Ihren Fingerabdruck und eine App, um auf Ihr Konto zuzugreifen.

Ist die zweistufige Authentifizierung schwierig?

Sie sind sich nicht sicher, wie Sie die zweistufige Authentifizierung für Ihre Accounts einrichten können? Die am häufigsten genutzten Dienste bieten eine Form der zweistufigen Authentifizierung an und haben dazu eine kurze Anleitungssseite.

Mehr Informationen unter [safeonweb.be/2FA](https://safeonweb.be/2FA).

Ist sie einmal aktiviert, können Sie fortan beruhigt schlafen.



einfach



schnell



extrem  
sicher