## Wie richtet man die Zwei-Faktor-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.be

## 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.
- Schließlich ebenfalls Ihre sozialen Netzwerke.

**Machen Sie es sich zur Gewohnheit, 2FA überall dort 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 Zwei-Faktor-Authentifizierung erfahren?

Surfen Sie auf **safeonweb.be**


Schützen Sie Ihre Online-Accounts mit der Zwei-Faktor-Authentifizierung.
Surfen Sie schnell auf **safeonweb.be**

CENTRE FOR CYBERSECURITY BELGIUM
febelfin
CYBER SECURITY COALITION
.be
Safeonweb.be


## Wie kommen Betrüger an meine Passwörter?

Die Verwendung von starken Passwörtern ist notwendig, aber dies alleine schützt Sie nicht ausreichend. Passwörter werden nämlich von Betrügern gestohlen oder erraten. Oder aber entlocken Betrüger Ihnen Ihre Passwörter durch miese 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.

## Zwei-Faktor was?

Die gute Nachricht ist, dass Sie so etwas vermeiden können, indem Sie, wann und wo auch 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 Zwei-Faktor-Authentifizierung, oder „2FA“. Im Grunde genommen kennen Sie das schon: itsme ist eine Form der 2FA, und der Digipass beim Online-Banking ist ebenfalls ein zweiter Schlüssel.

Safeonweb.be

## 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 Multi-Faktor-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 Authentifizierungs-App, um auf Ihr Konto zuzugreifen.

## Ist die Zwei-Faktor-Authentifizierung schwierig?

Sie sind sich nicht sicher, wie Sie die Zwei-Faktor-Authentifizierung für Ihre Accounts einrichten können? Die am häufigsten genutzten Plattformen bieten eine Form der Zwei-Faktor-Authentifizierung an und haben dazu eine kurze Anleitungsseite.

**Mehr Informationen unter safeonweb.be/2FA**.

## Ist sie einmal aktiviert, können Sie fortan beruhigt schlafen.

**einfach**

**schnell**

**extrem sicher**