

Halten Sie Cyber-Kriminelle fern

Schützen Sie Ihre Online-Konten mit einer Zwei-Faktor-Authentifizierung

ZWEI-FAKTOR WAS?

Die Zwei-Faktor-Authentifizierung oder 2FA ist eine Sicherheitsmaßnahme, um zu verhindern, dass Hacker oder Betrüger auf Ihre Konten zugreifen, indem sie zwei verschiedene Arten der Identifizierung verwenden.



DIES IST AUF DREI ARTEN MÖGLICH:



IHR PASSWORT ODER IHREN PIN

Etwas, das nur Sie kennen.



EIN CODE, DEN SIE AUF IHREM TELEFON ODER IN IHRER AUTHENTIFIZIERUNGS-APP ERHALTEN

Etwas, das nur Sie haben.



IHR FINGERABDRUCK, IHR GESICHT, IHRE IRIS,...

Etwas, das nur Sie sind

WARUM?

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 AKTIVIEREN?



Gehen Sie in die Sicherheitseinstellungen des Accounts, den Sie absichern möchten.



Suchen Sie nach der Option um 2FA zu aktivieren, und wählen Sie sie aus.



Wählen Sie den zweiten Faktor, den Sie verwenden möchten (z. B. SMS, Authentifizierungs-App usw.).



Folgen Sie den Anweisungen auf dem Bildschirm, um den zweiten Faktor zu konfigurieren.



Testen Sie, ob alles richtig eingestellt ist, indem Sie sich abmelden und mit dem zweiten Faktor erneut anmelden.

MÖCHTEN SIE MEHR ERFAHREN?

Surfen Sie auf safeonweb.be