Hoe stel je tweestaps-verificatie in?

Het instellen van 2FA verschilt per platform, maar over het algemeen zijn de stappen vrij gelijkaardig:

1. **Ga naar de beveiligingsinstellingen** van de account die je wil beveiligen.
2. **Zoek** naar de optie om **2FA** in te schakelen en selecteer deze.
3. **Kies de tweede factor** die je wilt gebruiken (bijvoorbeeld sms, authenticatie-app, etc.).
4. **Volg de instructies** op het scherm om de tweede factor te configureren.
5. **Test** of alles goed is ingesteld door uit te loggen en opnieuw in te loggen met de tweede factor.

Safeonweb.be

Waar beginnen?

- Begin met je e-mail
- Activeer het vervolgens op de websites waar je ook je bankgegevens achterlaat: webshops, booking websites, websites waar je tickets reserveert,...
- Je sociale media

Maak er een gewoonte van om het te gebruiken, overal waar het kan.

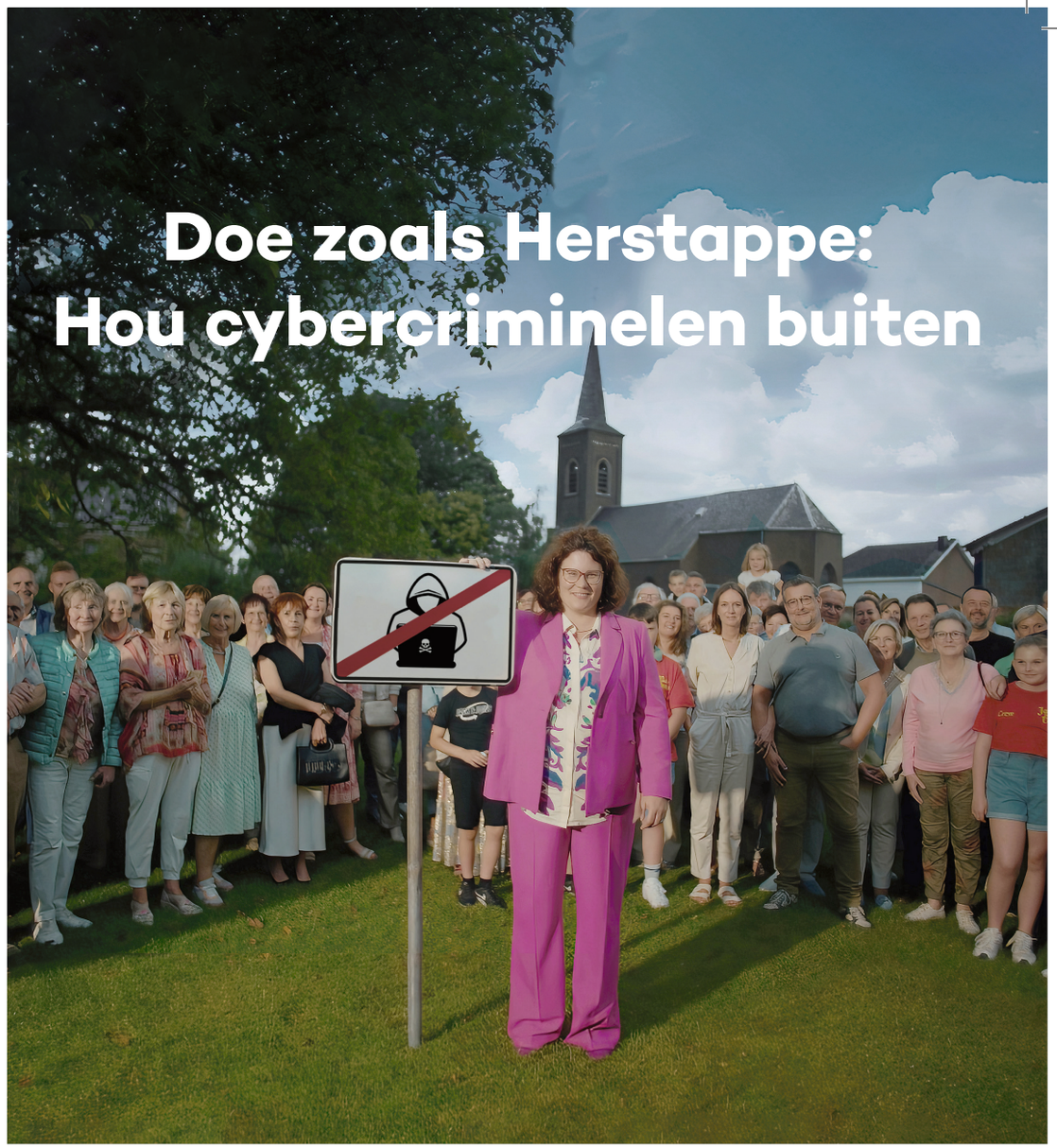
Hulp nodig?

Aarzel niet om familie of vrienden in te schakelen om je te helpen. Ook bij één van de vele Digipunten in Vlaanderen en in Brussel kan je terecht met je vragen.

Meer weten over tweestapsverificatie?

Surf naar **safeonweb.be**

Doe zoals Herstappe: Hou cybercriminelen buiten



Bescherm je online accounts met tweestapsverificatie.
Surf snel naar **safeonweb.be**

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

Safeonweb.be

Als een hacker of oplichter je wachtwoord kan bemachtigen, kan die:

- je mailbox gebruiken
- in jouw plaats gamen op jouw account
- bestellingen plaatsen in jouw naam
- iets op jouw Facebook plaatsen, enz...

Hoe komen fraudeurs aan mijn wachtwoorden?

Sterke wachtwoorden gebruiken is noodzakelijk, maar wachtwoorden alleen beschermen je niet voldoende. Wachtwoorden worden gestolen of geraden door oplichters. Of ze ontfutselen ze met een list (ze vragen ze met een smoesje aan de telefoon, of ze overtuigen je om ze in te vullen op een valse website). De kans dat één van jouw wachtwoorden nu al op het internet zichtbaar is, is redelijk groot.

Tweestaps watte?

Het goede nieuws is dat je dat kan voorkomen door altijd en overal waar het kan een 2de sleutel te gebruiken naast een wachtwoord: bv. gezichtsherkenning of een vingerafdruk, een code die naar je gsm wordt gestuurd. Een oplichter kan je wachtwoord bemachtigen, maar dat is waardeloos zonder de 2de sleutel. Dit heet tweestapsverificatie of 2FA. Eigenlijk ken je dit al: Itsme is een vorm van 2FA, als je een digipas gebruikt bij online bankieren, is dat ook een 2de sleutel.

Safeonweb.be

Om toegang te krijgen tot je account moet je bewijzen dat je bent wie je beweert te zijn.

Dat kan op 3 manieren of met 3 factoren:

1. met **iets dat jij alleen weet** (jouw wachtwoord of pincode),

2. met **iets dat jij alleen hebt** (een code die je ontvangt op jouw telefoon of authenticatieapp),

3. met **iets dat jij bent** (jouw vingerafdruk, gelaat, iris...).

Meestal gebruik je één van deze factoren, vaak een wachtwoord, om te bewijzen wie je bent, maar het is beter om 2 of meer factoren te gebruiken: dit is twee- of meerstapsverificatie (2FA of MFA). Je gebruikt dan bv. een wachtwoord en je laat daar bovenop ook een code naar je GSM sturen, of je gebruikt je vingerafdruk en een app om toegang te krijgen.

Tweestapsverificatie, is dat moeilijk?

Weet je niet hoe je tweestapsverificatie invoert op je accounts? De meest gebruikte diensten bieden een vorm van tweestapsverificatie aan en hebben een korte instructiepagina.
Meer info op safeonweb.be/2FA.

Activeer het één keer, en je kan op beide oren slapen.

eenvoudig

snel

bijzonder veilig