How do you set up two-step verification?

Setting up 2FA varies from system to system, but generally the steps are pretty similar:

1. **Go to the security settings** of the account you want to secure.
2. **Look** for the option to enable **2FA** and select it.
3. **Choose the second factor** you want to use (e.g. sms, authenticator app, etc.).
4. **Follow the on-screen instructions** to configure the second factor.
5. **Test** that everything is set up correctly by logging out and logging back in using the second factor.

Safeonweb.be

Where to start?

- Start with your email account
- Then activate 2FA on websites you use your bank details for: online stores, booking websites, etc.
- Your social media accounts

Make a habit of using 2FA wherever you can.

Need help?

Don't hesitate to ask family or friends to help you. You can also go to one of the many Digipunten / Espaces publics numériques if you have questions.

Learn more about two-step verification?

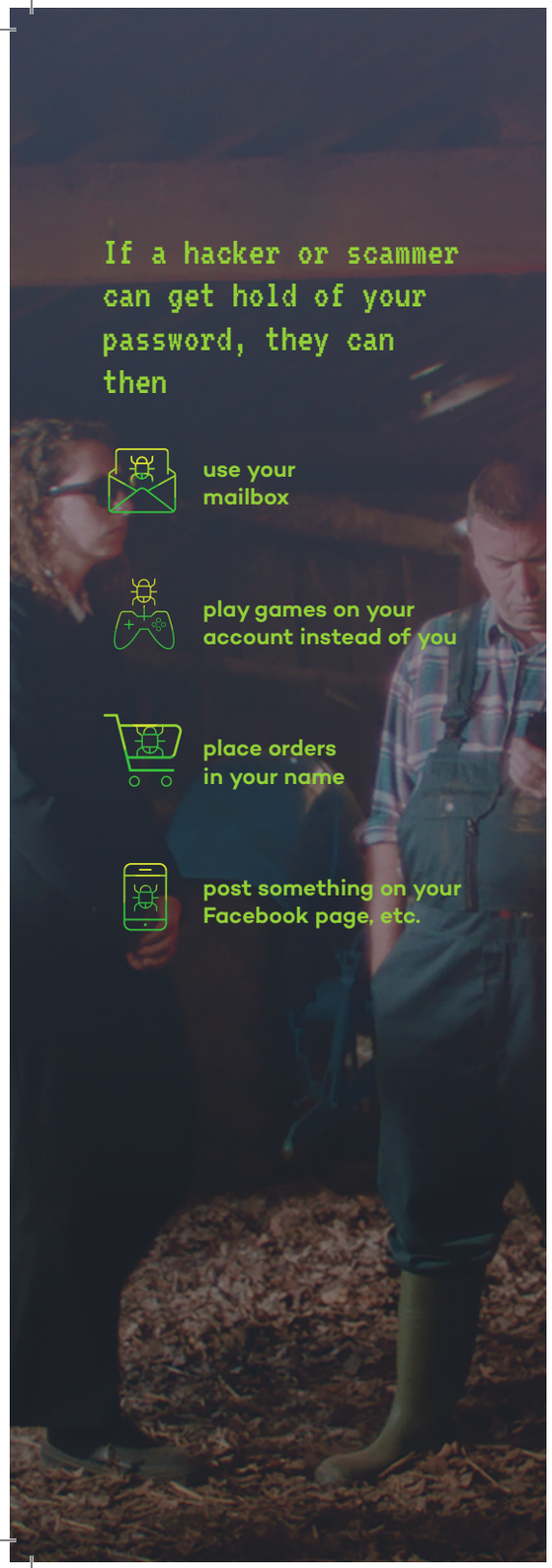
Surf to **safeonweb.be**

Do as Herstappe does: keep cybercriminals out!

Protect your online accounts with two-step verification.
Surf quickly to **safeonweb.be**

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

Safeonweb.be



If a hacker or scammer can get hold of your password, they can then

- use your mailbox
- play games on your account instead of you
- place orders in your name
- post something on your Facebook page, etc.

How can scammers get my password?

Using strong passwords is smart, but passwords alone do not provide sufficient protection. Passwords can be stolen or guessed by scammers. Or they can trick you into giving them your password: they will ask for your password over the phone under false pretenses, or you submit your password on a fake website. It's almost certain that one of your passwords is currently circulating illicitly on the internet.

Two-step what?

The good news is that you can prevent this by always using a second key in addition to your password such as facial recognition or a fingerprint or a code that is sent to your smartphone. A scammer can get hold of your password, but it is worthless without the second key. This is called two factor authentication, two step verification or 2FA. You may already know this system: "Itsme" is a form of 2FA or if you use an electronic card reader for online banking, this is also a second key.

Safeonweb.be

To access your account, you must prove that you are who you say you are.

You can prove this in three ways or using three factors:

1. using **something only you know** (your password or PIN code)),

2. using **something that only you have** (a code that is sent to your phone or an authentication app),

3. using **your own body** (our fingerprint, face, iris, etc.).

Typically, you only use one of these factors, usually a password, to prove who you are, but it's better to use two or more factors: this is called two- or multi-factor authentication (2FA or MFA). For example, you use a password and have a code sent to your mobile phone, or you use your fingerprint and use an App to gain access.

Two-step verification, is it difficult?

Not sure how to implement two-step verification on your accounts? The most commonly used services offer some form of two -step verification and have a short instruction page. **More information on safeonweb.be/2FA**.

Activate it once and you need never worry again.

simple

fast

extremely secure