

Keep cybercriminals out!

Protect your online accounts with two-step verification

TWO-STEP WHAT?

Two-step verification or 2FA is a security measure to prevent hackers or scammers from gaining access to your accounts by using two different forms of identification.

YOU CAN PROVE THIS IN THREE WAYS



YOUR PASSWORD OR PIN CODE

Something only you know.



A CODE THAT IS SENT TO YOUR PHONE OR AN AUTHENTICATION APP

Something that only you have.



YOUR FINGERPRINT, FACE, IRIS, ETC.

Your own body.

WHY?

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 TO ACTIVATE?



Go to the **security settings** of the account you want to secure.



Look for the option to enable **2FA** and select it.



Choose the **second factor** you want to use (e.g. sms, authenticator app, etc.).



Follow the **on-screen instructions** to configure the second factor.



Test that everything is set up correctly by logging out and logging back in using the second factor.

LEARN MORE ABOUT TWO-STEP VERIFICATION?

Surf to safeonweb.be