

Phishing test

Do you recognise suspicious messages? Discover whether you would fall into the trap of internet criminals. Are you an expert? Or could you use some more training? Take the test on **SAFEONWEB.BE**

YOU RECOGNISE
A SUSPICIOUS
MESSAGE. WHAT
SHOULD YOU DO?

Immediately send it to suspicious@safeonweb.be, don't click on links and don't enter any personal information.



TOO LATE! YOU
PASSED ON YOUR
DATA. NOW WHAT?

Warn your friends if you sent them a fake message. Change your passwords immediately and notify your bank and CardStop if you've passed on your bank details.

Relax!

And think twice before clicking on a link



RECOGNISE SUSPICIOUS
MESSAGES IN TIME AND
SEND THEM TO
SUSPICIOUS@SAFEONWEB.BE

“Relax and think twice before clicking on a link”



What is phishing?

Phishing is a form of online fraud using malicious emails, websites or messages. Cybercriminals try to take advantage of something you believe in or someone you trust. They also play on people's fear. Don't be fooled!

How do you recognise suspicious messages?

Phishing messages::

- are usually **unexpected** and you get them for no reason
- are coercive or arouse your curiosity
- contain **language errors** or have a strange writing style
- have a **vague contact title** or use your email address instead of your name
- come from an unknown sender
- contain a link that doesn't lead to a safe website

Not only emails can be malicious messages. More and more scammers try to make their move using fake text messages. This phenomenon is called **Smishing**. You can also receive phishing messages via social media such as Facebook and WhatsApp.