

Want to know more about phishing?

For all info, tips and a digital health test, go to safeonweb.be.

A great tip to start off with

Always keep your passwords and codes to yourself.
NEVER pass on passwords, bank card codes or response codes via e-mail, phone call, text message, or social media.



Download the Safeonweb app

Our app **warns you about cyber threats** and new types of online scams. So don't delay: download it from an official app store today.



Download the
Safeonweb app.

MORE INFO ON
SAFEONWEB.BE




Outsmart a phisher



Download the Safeonweb app.

Check safeonweb.be

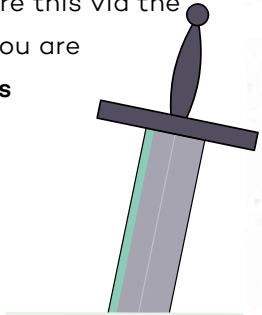


Do you ever receive suspicious messages?

An e-mail with an offer that seems too good to be true or a text message that looks like it comes from your bank? You are not alone: we are being flooded by a tsunami of suspicious messages. Fortunately, we often outsmart the scammers, but their messages are sometimes so misleading that many people fall into their trap.

Want to outsmart the scammers?

This is what you can do

1. Learn to recognise suspicious messages with the **tips on safeonweb.be**
 2. **Make it difficult for scammers:** don't click on links too quickly, never pass on codes and don't download files without double-checking first.
 3. Forward suspicious messages to suspicious@safeonweb.be.
- 

4. **Download the Safeonweb app** so that you are always up to date with the latest types of scams.
5. **Notify friends and family** who may be a little less attentive than you.

This is what we do at Safeonweb

1. We take the **fake links** from the suspicious messages that you send to **suspicious@safeonweb.be** and have them blocked, to protect less attentive internet users.
2. We also collect information about common **suspicious messages** and share this via the Safeonweb app. This means you are **quickly informed of suspicious messages** that are doing the rounds.



Have you already forwarded such info? Oops!

What now?

- If you have provided bank details, notify your bank immediately and **block your bank card** via **Cardstop**.
- If you have shared a password, immediately **change this password** everywhere you use it.
- If the phishing message has been forwarded to your contacts, **let them know**.
- **Report it** to the local police.

MORE INFO ON
SAFEONWEB.BE

