

Learn how to protect

yourself against fraud



do your thing

As an online bank, ING is always offering new digital tools to handle your banking. Online banking is easy and gives you more time to do what matters to you. Regardless, you might not feel entirely secure when working with the app or another online tool.

We can assure you that there is no need for concern: at ING, we do everything we can to keep our digital channels secure for you. However, security is something we do together. Below, we will run you through a few pointers on how to stay safe online, how to recognise online fraud and how to protect yourself against it.

Phishing

Phishing refers to fake e-mails containing a link through which criminals will try to obtain your confidential data. This data may include the numeric codes created with your ING card reader, your PIN code or the number of your debit or credit card. Once they've got these details, criminals will be able to make payments from your account.

Protect yourself against phishing

- ING messages are always personalised: they are in your preferred language and they contain your first name and/or surname.
- Check the sender of the message (e-mail address). ING's e-mail addresses always end in ing.be or ing.com.
- **ING will never ask you for confidential information**, such as your PIN code or the numeric codes generated by your card reader. You should never share this information by e-mail or over the phone.
- Any links in ING messages will always take you to ing.be
- Check the link by hovering over it with your mouse. Find out how to recognise fraud on ing.be/fraude
- You should only ever log on via the Home'Bank or Business'Bank start page on ing.be, and never via a link in an e-mail. Make sure you never share your secret code!

Smishing

Sometimes, fraudsters use text messages or WhatsApp/ Facebook Messenger messages to cause panic and make you act quickly. Often, these messages will contain an urgent warning to persuade you to click the link.

Protect yourself against smishing

We have changed our guidelines to deal with this type of fraud. From now on, **ING will no longer send text messages containing clickable links**. If you do receive a message with a clickable link, it did not come from ING, you do not click the link.

Fraud via online marketplaces

Say you're selling some clothes on an online marketplace. A potential buyer might contact you via a different platform than the one offered by the online marketplace in question (WhatsApp or Facebook Messenger, for example). The buyer might ask to pay via a different platform than the online marketplace. Everything might seem perfectly fine, until you realise they've cleared out your bank account!

Protect yourself against fraud via online marketplaces

- Always carefully read the security tips provided by the marketplace in question.
- Never accept a proposal from a potential buyer to finalise the sale outside of the marketplace.
- Never make a payment using a tool you're not familiar with.
- **If you've got any doubts, withdraw from the transaction immediately. It's better to lose a buyer than all of your money!**

Stay up to date via ing.be/fraude

We regularly publish information about the latest forms of fraud. Visit ing.be/fraude to find out how to recognise them and protect yourself against them.

Victim of fraud?

- Block your bank card via Card Stop on **+32 70 344 344**.
- Call us immediately on **+32 2 464 60 04**. We are available between 08:00 and 22:00 Monday to Friday and between 09:00 and 17:00 on Saturday.
- If you've spotted a suspicious transaction in your bank account, send us a message via fraude@ing.be
- If you've received a fraudulent message pretending to be from ING, forward it to us via (phishing@ing.be).
- For credit card fraud, report any fraudulent purchases via mijnkaart.be

Now that you've got all the info you need to protect yourself, make sure you install the new **ING banking app** via the App Store or Google Play today.



- ING is doing everything it can to guarantee the security of your online transactions and protect your privacy.
- All our online banking digital channels are part of a fully secure environment.

