# Scammers: common practices

Scammers try to mislead you by posing as trustworthy institutions, such as your bank. They put pressure on you to hand over money or access your account. Pay close attention to red flags, such as unexpected messages and urgent requests. And learn to recognise suspicious situations.

### **Examples of how scammers operate**

 You get a phone call from someone claiming to be from ABN AMRO. The caller tells you there is something wrong with your account and claims it is urgent that you transfer your money to a secure account.

This is a clear red flag! We never ask you to transfer money.

- You get an email from ABN AMRO telling you that your debit card will soon
  expire. However, it goes on to say that you can request a new one immediately
  via a link in the email. When you click the link, you are taken to a website. Once
  there, it says that to apply for your card, you only need to fill in your bank details.
  - Don't do it! We never ask you to request a debit card via a link in an email. We also never ask you to send or give your debit card to another person.
- You get a call from someone claiming to be from ABN AMRO. The caller tells
  you that it is currently unsafe to do your banking on your computer because it
  has contracted a virus. But then they say: Don't worry! One of their 'colleagues'
  can visit you later today to fix it. The only thing is that you will need to give this
  person your debit card, PIN, and login details.
  - Don't do it! We will never ask you for your security codes (such as your PIN and login details). We will also never collect jewellery, money, or other valuables to 'keep them safe'.

You can find more examples of 'What scammers often do' at abnamro.nl/securebanking. Do you think you might be dealing with scammers? Call us at 088 226 26 12 (no menu).



# Don't fall for fraud

Imagine it happening to you: becoming a victim of fraud and losing your money. But there are extra steps you can take to protect it: take advantage of our security tools and make it harder for scammers to steal your money.

## **Security tools**

Our security tools are free of charge and easy to enable.

#### Savings Lock

Scammers who contact you want only one thing: to steal your money as quickly as possible. However, if you have Savings Lock enabled, it will take 24 hours before you can transfer money. This means scammers can't pressure you into immediately withdrawing funds from your savings account. This gives your money an extra layer of protection.

You can enable Savings Lock in the ABN AMRO app or Internet Banking.

#### Debit card limit

Your debit card has a limit. This limit is for the amount of money you can spend per day or that you can withdraw from a cash machine. Don't set your card limit too high. This will prevent you from losing a lot of money should your debit card be stolen.

You can alter your debit card limit in the ABN AMRO app or Internet Banking.

#### • Daily transfer limit

Your daily transfer limit is the total amount of money you can transfer per day using the app. This applies to payments via iDEAL, payment requests, and bank transfers. Don't set your daily transfer limit too high. This will prevent you from being pressured into transferring large amounts of money to a scammer.

You can only alter the 'daily transfer limit' in the ABN AMRO app.



You can find more information on our security tools at abnamro.nl/eliminate-fraud.

Do you think you might be dealing with scammers? Call us at 088 226 26 12 (no menu).