# Red Flags in Scams

Recognise the signs. Take your time. Play it safe.

ABN·AMRO

# The tricks change, the signs don't

This is the ABN AMRO 'Red Flags in Scams' guide. In a world full of digital dangers, one thing remains unchanged: you are in charge of your own account. No one can access your money without your permission. However, scammers know this too, which is why they target you.

In recent years, digital fraud has got smarter and better organised. Scammers no longer need technical knowledge – they can simply buy software and stolen data online. Using the information from data breaches, they can create reliable profiles of their victims. And using artificial intelligence (AI), they can make fraudulent messages more personal and virtually mistake-free. As a result, it has become very difficult to distinguish the fake from the real.

But while the techniques may be harder to recognise, the signs are not. The red flags in this guide do not concern new technology, but are about behaviour that has been the same for years. After all, the way that scammers try to mislead you doesn't change.

Scammers know that people tend to be quick to trust others, and they take advantage of that. They try to put you under pressure or draw you away from a secure environment. And the longer a conversation lasts, the harder it is to stop.

Protecting yourself against fraud starts by recognising the signs: something happens that makes you feel pressure or doubt. That is the moment you should stop. Because remember: you are **always** allowed to check. And as soon as you recognise a red flag, hang up the phone and do not click on any links. Contact your bank, company, or institution yourself using the phone number on their official website or via their app.

## All red flags at a glance

| | |
|---|---|
| Red Flag 1: | An unexpected caller insists you must take action right now |
| Red Flag 2: | You are (almost) immediately asked to leave the website or app you are currently on and continue the conversation in another environment |
| Red Flag 3: | Something seems too good to be true |
| Red Flag 4: | You are told to read a script |
| Red Flag 5: | After you have been scammed, an unknown person gets in touch and offers to help you get your money back |

## Red Flag 1

# An unexpected caller insists you must take action right now

### Sign

Someone calls unexpectedly and says that your money is in danger. Or you get an email or text message with a link to an outstanding bill that you are told you must pay straightaway. The key sign of this scam is that you are always told to take action right now.

### Feeling

You feel panic and anxiety. You think you must act quickly to prevent things from getting worse.

### Why this is not true

No bank, company or institution will ever contact you out of the blue and tell you that your bank account is in danger. Nor that you have an outstanding bill you know nothing about. Also, you will never have to pay or transfer money straightaway – there will always be time to check or verify any payments. And your bank will never send you a link to pay via text message or email.

### What to do

Hang up the phone and do not click on any links. Look up the phone number of the bank, company or institution that are in contact with you, and call them back using that number. You will always be able to do this in your own time. And you can often call your bank directly through your banking app.

## Red Flag 2

# You are (almost) immediately asked to leave the website or app you are currently on and continue the conversation in another environment

### Sign

You start talking to someone via a website or app. The person you are talking to then quickly asks to continue the conversation in another environment, such as via a messaging app, email or phone. In other words, away from the website or app you are currently on. At this new location, they then ask you to make a payment.

### Feeling

The reason they give seems logical or convenient, so you understand why they are asking you to do this.

### Why this is not true

An official website or app is a secure environment. It has built-in security measures to protect you. Scammers will therefore try to persuade you to go to another environment where they are in control. Away from the official website or app, they can operate more freely. This also makes it harder for you to see that you are dealing with a scammer.

### What to do

Are you using a website or app? Then first read carefully how it works and check what it does to guarantee your security. Only communicate and pay via that same website or app. Is someone asking you to connect with them away from that secure environment? Don’t do it. Stop the conversation and report that person to the official website or app.

## Red Flag 3

# Something seems too good to be true

### Sign

You get a message saying that you have won a prize. Or you get an unexpected offer, like a huge discount on a product, an investment opportunity promising big money, or a high-salary job available for a small application fee.

### Feeling

You are excited. You think: What luck! This is my big chance!

### Why this is not true

Scammers use that feeling of excitement. They make the offer sound great, so that you don't think too carefully about it. But situations in which people get valuable things for free or are guaranteed to win big money almost never happen in real life. Does something sound too good to be true? Then stop and think. Check to make sure that it's genuine.

### What to do

Look up the company or the offer. Do this from different places on the internet. And be warned: scammers can create fake websites and reviews. That's why it is not enough to look at just one website. Does the offer concern investments? Then check out the website afm.nl to see if a company is real. (The AFM is the official supervisor for banks and investors in the Netherlands.) Also, go to independent websites to read about other people's experiences. And ask a friend or family member to take a look with you.

## Red Flag 4

# You are told to read a script

### Sign

You get an unexpected call. The person on the phone claims to be from the bank or from a company or organisation. You are told that your money is in danger and that you will be contacted shortly by someone else from the bank. You then get an email in advance containing text that you are supposed to read aloud. Or they might tell you to write down what you need to say to the bank later. However, this entire story is almost never true.

### Feeling

What you are told is full of details and sounds convincing. You think: This person knows exactly how things work, so it must be correct.

### Why this is not true

No bank, company or institution will ever ask you to tell a story that might not be true, nor to withhold information. So if someone tells you what to say, that is a red flag. You are dealing with a scammer.

### What to do

If someone dictates what you are supposed to say or asks you to read a script, hang up immediately. Then call your bank yourself through your banking app or the number on the official website. Tell them what happened.

## Red Flag 5

# After you have been scammed, an unknown person gets in touch and offers to help you get your money back

### Sign

You were scammed and you now feel despair and embarrassment. Then you get a message from someone who claims they can get your money back. This person might say they have a lawyer or that they can recover the money. They might even say that they have contacts in the police. However, if you want their 'help', it will cost you some money.

### Feeling

The message gives you hope. You want your lost money back and you think: At last, someone who can help me!

### Why this is not true

Any bank, company or institution that is trying to retrieve your lost money will never ask for extra payment upfront. The police also never ask people for money to solve a case.

### What to do

End the contact immediately. Do not trust any promises that are made. And be warned: these scammers know that you have been scammed before. This means they will often try again. So call your bank yourself. Use the app or the phone number on the official website. Tell them that someone has called you or is sending messages again.

260135