The ABC of Scams

Different types of scams explained in simple terms.

By: ABN AMRO, 2025

ABN·AMRO

Introduction

Scammers use all kinds of tricks to get money.
Some tricks have been around for a long time. Others are new.
Sometimes victims are approached in person.
But more often it's done by phone, email, text message, or app.

It is important to know how scammers operate.
That way, you might notice when someone is scamming you.
Scammers' tricks sometimes have complicated names.
It can be difficult to understand how a scam works.
That is why we have created this list using simple terms.
This list describes many different types of scams.

The names of these scams might still be complicated.
But you don't have to memorise them.
The most important thing is for you to recognise the scammers' tricks.
Then there is less chance of you falling victim to them.

Did something happen that didn’t feel right?

Do you think you’ve been scammed?
Have you experienced anything unusual?
Then contact your bank immediately.

You can call us through the ABN AMRO app.
If you use the app, you will be immediately put through to the correct department.
It is secure and fast.

Would you rather call by phone? That is also possible.
Call 0900 - 00 24.

Calling from abroad? Then you can call +31 10 241 17 20.

All these calls are charged at the usual rate of your phone provider.

If you have been scammed, you can also report it on abnamro.nl/reportingfraud.

List of scammers' tricks

B

Description of **bank helpdesk scam**:

You get a call.
The person on the phone claims to work for your bank.
They might say, for example, that something is wrong with your account.
They advise you to transfer your money to another account that is safer.
They might also ask you to give them your PIN or allow them to take over your computer.
This is a trick to steal your money.
The person calling does not work your bank. They are a scammer.
And if you transfer the money, it will go to this scammer's account.

Description of **boiler room scam**:

You get a phone call or an email.
Someone says they have a special opportunity for you.
You don't want to miss out. It could be worth a lot of money.

The person calling or emailing might ask you to invest in a project.
They often know details about you.
Enough to make you think you can trust them.
The person first asks for a small investment.
This often makes you an immediate profit.
That is why people are tempted to invest even more money.
But the person calling or emailing you is a scammer.
The money you eventually invest goes directly to them.
And often, the project you're investing in doesn't exist.

C

Description of **crypto scam**:

Someone asks you to invest in a cryptocurrency like Bitcoin.
They use videos or commercials that feature celebrities.
You're told that you can make a lot of money in a short time.
When you invest, it seems like you'll make an immediate profit. Sometimes you actually do.
This often gets people to invest even more.
But it's all fake.
The person who contacted you is suddenly unavailable.
And your money has gone to scammers.
This is cryptocurrency investment fraud. Sometimes called a crypto scam.

D

Description of **dating scam**:

You meet someone online through a dating site or social media.
You click with them. You exchange messages over time and build a bond.
After a while, the other person asks for money.
They say it's for an emergency, a sick family member or a plane ticket to visit you.
The other person asks you for money more than once.
But in the end, the relationship turns out to be fake.
The love was fake. The other person was a scammer.
You feel sad. You were lied to. And now, you've lost your money and your love.

Scammers use fake profiles, stolen photos, and false stories.
So you should be careful with people you meet online.
Especially if they are quick to ask for money or personal information.

Description of **debit card scam**:

You get an email, a letter, or a phone call.
You are told that your debit card is no longer working.
You are asked to send off your debit card.
Or to give it to someone who will come to pick it up.
This message looks like it comes from your bank. But it's not.
A real bank will never ask you to send off or give up your debit card.
And if you send off or give it up, your debit card will end up in the hands of scammers.
They will use your bank details to withdraw money from your account.

D

Description of **deepfake scam**:

Someone sends you a video that has you in it.
You're shocked because it looks real.
But it's fake. The video was created using artificial intelligence.
A scammer tells you to send them money.
If you don't, they threaten to send out the video.
You feel powerless, scared, and under pressure.

Sometimes your friends or family get a video in which it looks like you're asking for money.
This video is also fake.
If your friends or family send the money, it goes directly to the scammer.

This type of fake footage is used in a variety of scams.
It can happen with dating scams.
During a video call, your fake love interest appears real.
It can happen with CEO fraud.
This is when you seem to be in contact with an important person at a company.
It also happens with sextortion. We'll talk about this type of scam later.

F

Description of **fake job scam**:

You get asked if you are interested in a new job.
The job itself looks great.
But it's fake. The job doesn't exist.

The scammer pretends to be a prospective employer.
In that context, they might ask for personal information or a copy of your ID.
Sometimes they get you to click on a link that contains malware (a computer virus).
Sometimes they ask you to send payment for something, like training or a work pass.
After you have paid or shared your personal information, you hear nothing more.
The scammers now have your money or your personal information.

I

Description of **identity theft**:

You are contacted by a company or organisation.
It will be a company or organisation that you know.
They ask you, for example, to send them online a copy of your ID.
Months later, you are suddenly getting bills.
You have to pay for things that you never ordered.
A scammer has used your name, date of birth, address, or a copy of your ID.
With this personal information, the scammer can buy items or even open a bank account.
So you should always be careful when sharing your information. Especially online.

Description of **internet fraud**:

Internet fraud involves deception carried out online.
Perhaps you see the website of a trustworthy company.
Or you get an email from someone you know.
But it turns out to be fake. Created by scammers.

Scammers use clever tricks to mislead you.
You may think you're buying something from an online store or through Marktplaats.
Or you may think that you're helping someone.
But in reality, you're dealing with a scammer.
A scammer who is trying to use the internet to steal your money or personal information.

I

Description of **invoice scam**:

You receive an invoice or a fine.
It could also be a bill from the Tax Office.
The document states that you have to pay an amount of money.
It looks real. But it's fake.
If you transfer the money, it will go to scammers.
So check the document carefully before paying.

Sometimes a scammer will change the account number on a real invoice.
You might think you're paying a real company.
But even then, the money will go to the scammer.
Always check the invoice carefully. Did you really order the product stated?
And compare the account number on the invoice with your own purchase confirmation.

M

Description of **malware**:

You get an email with a link or attachment.
Or the link is on a text message or other type of message.
But if you click the link or download something, malware becomes active.

Malware is a computer virus.
Scammers can use it to access your laptop, phone, or tablet.
This happens without you even realising it.
Your devices often contain documents, passwords, or banking information.
That's what the scammers are looking for.
They can do various things with this information.
Such as stealing money from your account.

Description of **money mule**:

You get a message through a social media outlet like Snapchat or Telegram. Or you see a job opening.
The question is usually simple: 'Do you want to make some quick money?'
All you have to do lend out your bank account or debit card.
And you get paid in return.
It sounds like a quick and easy way to make money.

Money is put into your account.
You are asked to transfer part of it to another account.
And you can keep the remainder.
But this is not legal. In fact, you are assisting criminals.
Someone who does this is called a 'money mule'.
You can get fined. Or even go to prison.
And the chances of getting caught are very high.
The police and the banks are always alert to this practice.

P

Description of **phishing scam**:

You get an email.
It appears to be sent by your bank, the government, or a well-known company.
The email says that you need to act quickly, to log in or pay for something now.
When you click the link, you are taken to a website.
But this website is fake and your login information is stolen.
The scammers then use it to steal money from your bank account.

Description of **purchase scam**:

You see a great offer online.
Perhaps in an online store or on social media like Facebook or Instagram.
The price looks good, and you decide to pay.
But then your purchase never arrives, and the website disappears.
The seller was a scammer.
And your money is gone.

This is called a purchase scam.
You think you're buying from a real store, but it's not.
The online store is fake and using a real company's name.
And sometimes, even the company itself is non-existent.

Q

Description of **QR code scam**:

You want to buy or order something and you scan a QR code.
You are taken to a website where you have to enter your personal information.
You may trust the message or link, but the website is fake.
And the money goes to scammers.

Sometimes, this process also installs malware on your phone.
Scammers use this malware to access your personal information.
Then they can steal your money.
This is scam using QR codes. Sometimes this is called quishing.

Not every QR code is risky.
But when you scan a QR code, look carefully at what you see on your screen.
Only pay if it makes sense.

R

Description of **refund and recovery scams**:

After falling victim to a scam, you're contacted again.
Someone says they can help you get your money back.
Of course, you have to pay for this.
After you send the payment, you never hear from them again.
You have not been helped and have lost even more money.
In fact, you've been scammed again. This is a refund and recovery scam.

S

Description of **sextortion scam**:

You receive photos or a video.
You are in them.
The images are sexual and they shock you.
These images are usually fake.
Created using artificial intelligence.

The sender threatens to share the photos or video with your friends, family, or colleagues.
If you want to prevent that, you have to pay them.
You feel ashamed, powerless, and anxious. You often don't dare to talk about it.
But the fact that you don't want to talk about it is exactly what the scammers want.
This type of scam is becoming increasingly common, especially among young people.
It can cause panic, stress, and depression.

Description of **shouldering**:

You enter the PIN for your debit card or phone.
But unknown to you, someone is looking over your shoulder.
This might happen at a cash machine or the ATM at a supermarket.
It might even happen when you pay your bill at a café terrace.
After watching you, the scammer steals your phone or debit card.
Often before you realise it.
And knowing your PIN makes it easier for the scammer to steal your money.
This is shouldering, sometimes also called 'shoulder surfing'.

Description of **SIM swapping**:

A scammer calls your phone company using your name.
They know your full name, date of birth, and address.
The scammer asks the phone company to transfer your phone number to a new SIM card.
The scammer will then get your text messages, notifications, and codes.
They can now access your online accounts and sometimes even your bank account.

S

Description of **skimming**:

You pay using a PIN machine or withdraw money from a cash machine.
But these machines have had spyware installed.
Or set up with a hidden camera.
This is how scammers can acquire your personal information or PIN.
Which they can then use to withdraw money from your account.

Description of **smishing**:

You get a WhatsApp or text message with a link to a website.
It resembles a message from your bank or another well-known company.
But it's from scammers.
The scammers tell you to act quickly.
They do this on purpose, so you don't have time to think.
If you click the link, you will be taken to a fake website.
On that website, you will have to enter your personal information or transfer money.
But if you do, you will lose your money or your personal information.

Description of **social media scam**:

You get a message through a social media outlet like WhatsApp or Facebook.
The message appears to be from someone you know.
That person says they're in trouble and needs money quickly.
But this message is not from someone you know. It's from a scammer.
After you've transferred money, the scammer might ask for more.
And after that, you never hear from them again.
The scammer has disappeared, and your money is gone.
This is a social media scam. It also goes by other names.
Sometimes it's called the help request scam, WhatsApp scam, or friend-in-need scam.

S

Description of **spoofing**:

You get a call from someone.
They claim to work for an organisation like your bank, the government, or the police.
The real phone number appears on your screen.
This makes you believe that you're actually talking to, say, your bank.
You are told there is a problem.
Perhaps you are told that information is missing or you need to change something.
The scammers direct you to a fake website.
Once there, you have to enter your information or transfer money.
And that money goes to the scammers.
This is spoofing.