PAYMENT FRAUD AND BUSINESSES

How to recognise and prevent fraud

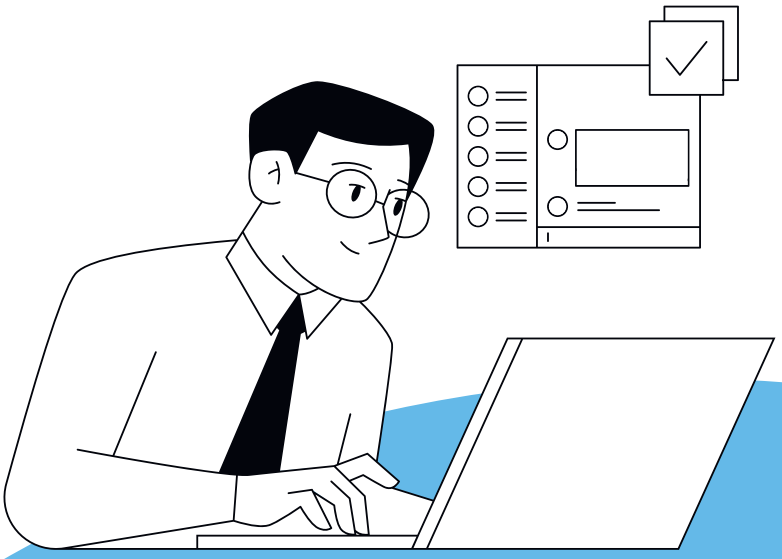
febelfin

Consumers are not the only victims of financial fraudsters; businesses are increasingly becoming targets for various forms of payment fraud too.

Several forms of fraud currently exist, targeting businesses, in particular, with the potential to cause massive financial losses. Examples include CEO fraud, invoice fraud, phishing, and more.
Although banks constantly invest in fraud detection systems and monitoring, detecting all fraud attempts is unfortunately impossible.

But even as a business, you can take your own initiatives to raise vigilance and set up your own security systems. Because we'll only be able to stop the fraudsters together.

Discover five common forms of business fraud in this brochure. We explain how fraudsters try to deceive and how you can protect yourself, your employees, and your business against them. And you'll find useful tips to detect or – ideally – prevent such fraud in your business.



Train your financial staff

Accounting staff are the first line of defence against payment fraud. They are the ones who can detect fraud and prevent financial losses. We recommend that you distribute this brochure in your business. Urge board members and all employees with authorisation to work on the business accounts to read it.

INVOICE FRAUD

— What is invoice fraud?

The name speaks for itself: in invoice fraud, fraudsters falsify or alter an invoice. They intercept a genuine invoice, replace the recipient's bank details with their own, and send the altered invoice. A business can receive a fake invoice, or send an invoice itself, which is subsequently falsified.

— How does invoice fraud work?

First, fraudsters intercept an invoice. This can happen in several ways:

- From the postal system: fraudsters take the invoices from the Belgian postal service's red post boxes or sorting centres.
- They steal invoices from private individuals' or businesses' letterboxes
- They hack into a supplier's IT system, intercept invoicing emails or change the account number. So be vigilant about invoices you receive electronically as well.

The fraudsters then change the recipient's account number.

- They often scan in the original invoice and alter the supplier's or vendor's details (account number and sometimes the telephone number) with special software.
- Alternatively, they include a letter with the invoice stating that the account number has changed. Sometimes they put a sticker on the envelope or the invoice itself saying 'Attention: change in account number'.

They send the altered invoice afterwards.

They sometimes also make fake invoices themselves.

TIPS TO PREVENT INVOICE FRAUD

- Compare the account number on the invoice with the account number on the vendor's or supplier's order form or official website.
- Be extra vigilant if an invoice mentions a new account number or if there is a sticker 'Attention: change in account number' on the envelope or invoice, even if it is the first invoice you receive from a vendor or supplier. Take a moment to verify the account number before paying.
- If you're in any doubt, call the business using the number already in your database, not the one listed on the invoice (which might also be fake).
- Keep a record of your suppliers' details and bank account numbers, even if you pay electronically. When you receive a new invoice, you can easily check whether the account number matches your records.
- If you receive an invoice that looks suspicious, do not pay it until you have properly verified that you are a customer of the business or have ordered something from them.
- If you receive the invoice by email, check that the email address is correct.

— I've paid a false invoice anyhow. Now what?

- Contact your business's bank as soon as possible to report the fraud. Your bank will ask the beneficiary's bank to refund the money. This bank will also try to block the transfer or account so that the fraudsters can no longer withdraw money.
- File a complaint with the police.
- Report it at https://meldpunt.belgie.be/meldpunt/en/welcome (option 'fraud and scams' > 'other problem'). At the end of your report, you'll be immediately advised what steps you can still take and who can assist you in that regard.

REACT QUICKLY

If you detect fraud after a transfer has been made, notify your bank immediately. A list of all contact points can be found at www.cardstop.be/content/cardstop-be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html.

If you notify the bank quickly, there is a greater chance of recovering the stolen money. If necessary, you will have to complete other formalities with the relevant authorities (filing a complaint with the police, and so forth). The experts at the banks can advise you on what steps to follow.

CEO FRAUD

— What is CEO fraud?

In CEO fraud or social engineering, fraudsters impersonate a company's CEO (or other internal or external person of trust) to manipulate an internal employee of that company into performing an action (often a payment) or revealing confidential information.

— How does CEO fraud work?

- Fraudsters **first gather information** about a company's internal payment procedures and the employees authorised to process large payment transactions. The fraudsters do this by contacting employees by email or telephone, posing as auditors or a government department.

- When the fraudsters have enough information, **they contact one or more employees responsible for payments** (such as accounting) and pose as the CEO. To do this, they usually hack into the CEO's mailbox or create a fake email address that closely resembles the CEO's real address. In this case, often one letter is changed in relation to the official address. The fraudsters then concoct a story requiring a large sum of money to be urgently transferred and urge the employee(s) to keep the matter strictly confidential.

- Sometimes the fraudsters take things a step further by involving a consultancy or a lawyer (whose identity they have assumed). The consultancy or lawyer will confirm the transaction and reiterate that the payment is urgent and confidential.

- Employees who fall into this trap unwittingly transfer large sums of money to the accounts of money mules, from which the money is then diverted to the fraudsters' accounts.

TIPS TO GUARD AGAINST CEO FRAUD

1. Always check the domain name in the sender's email address
2. Be wary of 'confidential' instructions to urgently transfer large sums of money.
3. If you receive such an urgent request, always call the person making the request back on a telephone number you know.
4. Never leave dual signatures to the same person (cards and PINs)
5. Build in sufficient control procedures:
   - Arrange for payments – and especially large ones – to not only be communicated by email but also confirmed by text message (SMS), a WhatsApp message, a phone call, and so on.
   - Designate another person within the company (not the CEO) whom employees can approach if they receive a confidential or urgent request. This person can then check with the CEO that the request is genuine. Note: no one outside the company must know who this designated person is.

— I fell into the trap. Now what?

- Contact the bank as soon as possible.
- File a complaint with the police.
- Inform your company's ICT department if the CEO's mailbox has been hacked. Fraudsters probably have access to a lot of information because of that mailbox and passwords, for example, will have to be changed.

PHISHING

— What is phishing?

Phishing is a technique in which fraudsters attempt to trick you into revealing your personal codes to gain access to your online banking environment. Phishing messages can vary widely in content. It could be a fake message (e.g. by email, WhatsApp or text message/SMS) from your bank to renew your bank card, from your phone operator about a problem with your subscription payment, from FPS Finance promising you a refund, and so on. However, this message always includes a link to a fake website. If you click on this and enter your business bank details and secret code on the fake website, you will grant the fraudsters access to your business accounts.

TIPS TO PROTECT YOUR BUSINESS FROM PHISHING

- Never provide online banking codes (codes generated by your card reader) by email, social media, text (SMS) or phone. Your company's internet banking codes are as secret as the PIN for your bank card!
- Never enter your bank's payment site or mobile app through a link. Your bank never asks for your codes through a link.
- Always type the address of your business banking website into your browser yourself. You can also save the address (URL) in your browser's favourites list or open the bank's mobile app yourself.
- If you have any doubts, it's better to stop. If you've received a message that seems strange and you're unsure about what is happening, assume the worst and stop everything.
- Be sure to take a look at the free training module 'Watch where you're going!' of 'Surf without worries' via Safeonweb.be.

— Did you fall into the trap anyhow?

- Contact your business's bank as soon as possible. The bank can be reached 24/7 to report online fraud on dedicated fraud numbers. A list of all contact points can be found at www.cardstop.be/content/cardstop-be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html/
- Once you have given your card details, notify Card Stop (www.cardstop.be or 078 170 170).
- Change your codes.
- File a complaint with the police.

SAFE DEPOSIT BOX FRAUD

Another form of fraud is emerging within businesses, known as safe deposit box fraud. A seemingly trustworthy sender (e.g., a social secretariat, a bank, a postal service, a telephone operator...) calls the company or self-employed person to warn that suspicious banking transactions are taking place on the company account. Damage can be prevented if you act 'quickly' and transfer the funds to a 'safe deposit box'. However, it later turns out that such a 'safe deposit box' does not exist and the manager is left with a major financial loss.

Safe deposit box fraud usually occurs in two steps. First, the fraudster sends a phishing message to gain access to the company's or self-employed person's account. Then, they call an employee of the company or self-employed person and convince him/her to transfer the money from the account to a so-called 'safe deposit box'.

— How does it work?

This type of fraud often starts with a phishing message that cyber criminals send by email, text message, WhatsApp or social media. This message contains a link that takes you to a fake website. Fraudsters use this website to collect personal information such as contact details or even codes for online banking services. Once the fraudsters have this information, they can start their fraudulent actions: they call the company or self-employed person and pretend to be a bank employee. They then explain that suspicious transactions have been made on the account.

Sometimes this step is skipped and fraudsters simply call the company or self-employed person with a lot of persuasion. They will do anything to gain trust.

The fraudsters will then offer to transfer the money to a safe account, namely the so-called 'safe deposit box'. But that type of account does not exist at all. And if the company employee or the self-employed person does transfer money to this false 'safe deposit box', it ends up in the account of a **money mule**. From then on, the transferred amount is transferred to the cyber criminals' account in record time.

An alternative scenario is that the fraudster has the 'cancellation of fraudulent transfers' confirmed by the victim, while in fact he or she just signs the fraudulent transfers.

TIPS TO PROTECT YOUR BUSINESS FROM SAFE DEPOSIT BOX FRAUD

- Never disclose personal information and/or bank codes (account number, PIN, response code) via email, SMS, phone call, social media message, or WhatsApp. Neither a bank nor any other organization will make such a request by phone, email, SMS, or social media.
- Banks will not advise you to transfer company money to a third-party account. The concept of a safe deposit box account does not exist!
- Banks will not ask you to install remote control software (AnyDesk, TeamViewer) on your computer.
- If you receive a suspicious message or call and doubt its authenticity, do not take risks and do not respond. Don't be influenced and convinced to act 'quickly.' Need more information? Call the bank yourself. Fraudsters cannot intercept this call, but they can 'spoof' a real phone number of the bank and call you via this number.

— Did you fall into the trap anyhow?

- Contact your company's bank as soon as possible. They are available 24/7 through special numbers to report online fraud. You can find an overview of all contact points **here**.
- Notify Card Stop (078 170 170).
- File a complaint with the police.

BANK HELPDESK FRAUD

— What is bank helpdesk fraud?

This type of fraud means that entrepreneurs are called by scammers who pretend to be a bank employee. They convince entrepreneurs to take over their computer screen and to receive their personal codes. This way, they succeed in stealing big amounts of money. This type of fraud is on the rise and can lead to major financial damage in no time.

— How does it happen?

The entrepreneur generally receives a call from a so-called employee (of the fraud department) of his/her bank warning that suspicious transactions have just been detected on the account of the company. The scammer convinces the entrepreneur about the emergency of the situation and gives them advice to prevent worse.

Once the victim is persuaded, they ask to transfer money to (non-existent) 'safe accounts' or the client/entrepreneur is asked to cancel (non-existent) fraudulent transactions together with the so-called 'bank employee'.

The entrepreneur is also prompted to install software (AnyDesk, TeamViewer...) that allows the so-called 'bank employee' to assist him/her. In this way, the scammer has the full control of the computer or smartphone of the client. The scammer decides what the entrepreneur can(not) see and is therefore able to log in to online banking and make bank transfers from the corporate and private accounts of the victim. The entrepreneur signs these bank transfers, thinking that these are destined to safe accounts or that he/she is cancelling these transactions.

HOW TO PROTECT YOURSELF AND YOUR BUSINESS

1. If you are called by a bank employee asking you to install software to take control of your computer, don't accept this and end the call immediately!
2. The enterprise can decide that employees may not install software.
3. Take the necessary measures: inform your colleagues, friends or employees about this so they can better arm themselves against this type of fraud.

— Got scammed?

- Contact your company's bank as soon as possible. They are available 24/7 through special numbers to report online fraud. You can find an overview of all contact points **here**.
- Notify Card Stop (078 170 170).
- File a complaint with the police.

A few more best practices for online payments in a business:

— Good dual signature management

Dual signatures are a way to prevent fraud. The second person signing is separate from the transaction and is more likely to notice the fraud.

— Sensible use of individual authorisations for actions on business accounts

Each authorised person must have individual access to the business accounts. After all, if they share electronic access to the business accounts with others, they not only share their authorisations but also provide access to their private accounts. Having individual access is safer for the business and for the employees themselves because they can only perform the transactions linked to their authorisations.

FINAL WORD

Any business can become a victim of fraud. Although fraud can take numerous forms, there are fortunately also many steps that can be taken to protect your business and employees from it. It remains essential to stay vigilant and take appropriate measures to keep fraudsters at bay.

Disclaimer: This brochure is purely informative and Febelfin cannot be held liable for any damage or loss that results from consulting or using the provided information.

Koning Albert II-laan 19, 1210 Brussels

www.febelfin.be