FINANCIAL FRAUD AND BUSINESSES

How to recognise and prevent fraud

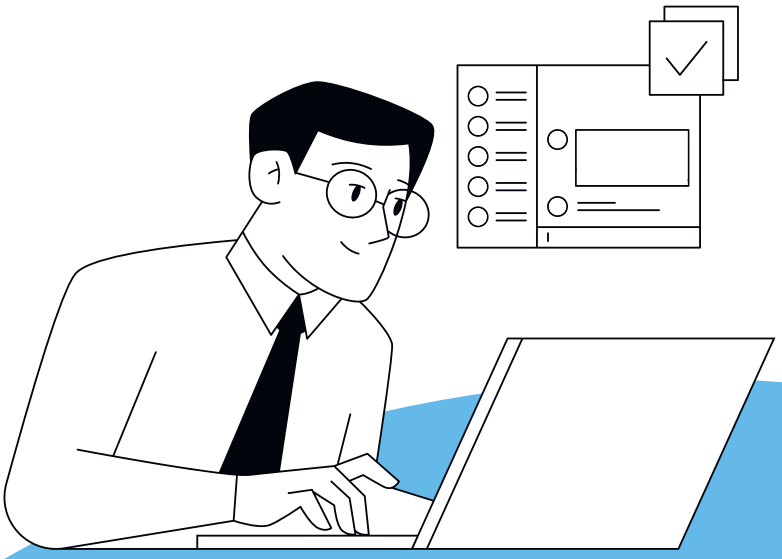
febelfin

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

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.

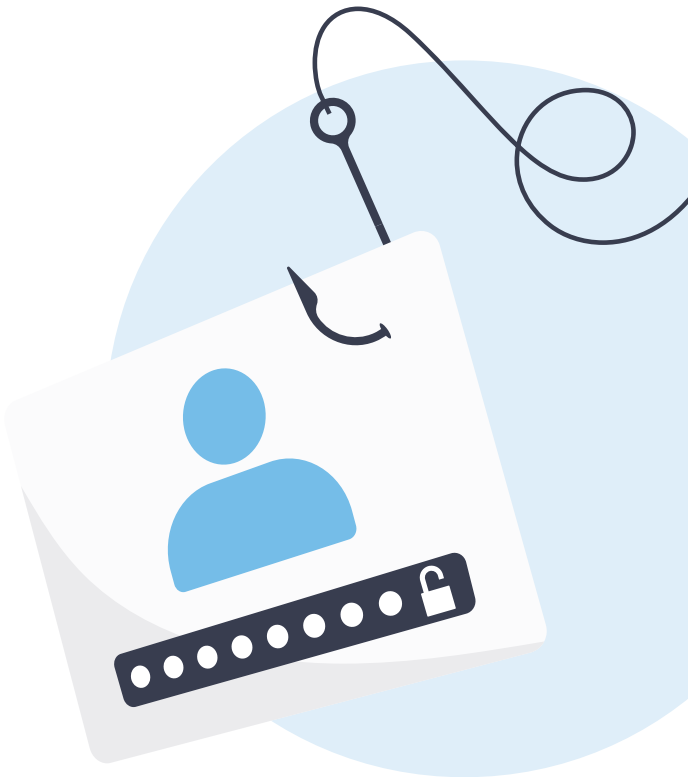
- Employees who fall into this trap unwittingly transfer large sums of money to the accounts of money mules, from which the money is then diverted to the fraudsters' accounts.

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.

— 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.

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. Never leave both signatures to the same person and check everything you sign.

— 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, 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