Safeguard your business against fraud

Corporate fraud – CxO fraud

This leaflet describes the most frequent fraud cases that could impact you and your employer. It also gives advice on how to protect yourself. Fraudsters are clever, well organised and masters in 'social engineering'. They use deception to manipulate individuals into divulging confidential or personal information to commit cybercrime. Fraud cases occur worldwide on a daily basis, and generate millions in losses. Beware.

How to use this document?

Distribute it within your company to raise awareness among employees, especially employees who are authorised to access you company's accounts or who can create and/or approve payment instructions. Fraudsters often target employees with such rights.

While there's no full protection against cybercrime, awareness can help recognise so-called 'red flags'.

Communicate and apply the recommendations in this leaflet to reduce the risks of fraud!

Important information!

If fraud is in progress, always notify your ING contact immediately. Although a transaction made is permanent, an attempt can be made to retrieve the funds before they disappear permanently from the beneficiary account. Speed is of the essence as with every minute passing, the chance of getting your transaction reversed will diminish.

If your ING contact is not available, please call

ING Wholesale Banking Fraud operations at +31 20 584 7840

After working hours or for a fraud that occurred in the past, please contact wb.fraudalert@ing.com

CxO fraud, what is it?

Social engineering is manipulating people so that they disclose confidential or sensitive information. A fraudster poses as a senior manager or a third party acting on behalf of senior management to manipulate employees into executing payment transactions or divulging confidential information.

What happens?

1. Fraudsters will contact your company by email or phone, acting as auditors, chartered accountants or even a government department undertaking an investigation. By doing that, they gather information on your company's internal payment procedures as well as on the people who are authorised to make them. Also, information on social media (LinkedIn, Facebook...) might help fraudsters to identify employees involved in payment procedures or identifying staff being away on holiday with the intention to impersonate them.
2. They contact company employees with rights to make large payments posing as the CEO, CFO or other senior manager, referring to a decision to possibly take over a foreign rival, or other event requiring a major transaction.
   Usually, in these scenarios the fraudster says that the transaction must be executed urgently and with the utmost secrecy.
3. The fraudsters may even refer to an external consultancy (whose identity they have stolen) to make the operation more credible. "The consultant" then contacts the target employee to confirm the transaction and reiterates the secrecy and urgency of the payment to be made. If the employee hesitates the fraudsters will use several tricks such as name dropping top executives in the company, flattery or even threats.

Variants of such fraud

Several varieties exist, such as fraudsters posing as lawyers, notaries, police officers, helpdesks, etc.

What safeguards to take?

- Always act cautious when funds are asked to be transferred urgently and secretly.
- In the event of an urgent request, always call the person who made the request back on a known, previously verified phone number.
- Implement segregation of duties like dual signing permissions, where at least two separate people have to sign payments. Also make sure that signing is always done properly, following company's protocol, not just sign off based on trust.
- Do not allow people to share authorisation devices (e.g. cards and PIN numbers).
- Ask employees to limit the level of detail in their social media expressions on the role they occupy within the organisation.