Safeguard your business against fraud

Corporate fraud – fake documents

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 daily 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:

- the ING emergency line (+31) 20 228 8800 (24/7).
- For a fraud that occurred in the past, please contact fraude@ing.com.

Fake document fraud, what is it?

Our business often requires documents to be shared to establish/validate relationships or transactions. Various parts of these interactions be exposed to fake or manipulated documents. The scope of this type of fraud is large as it may be isolated to a single document by a known partner, or as part of a more complex fraud attempt.

Red flags

Below is a list of questions you may ask when receiving a document:
- **signature** - does the signature match against your signature database?
- **paper** - does this feel like what you would expect?
- **language** - when dealing with international business, is this document arriving in the language that you expect?
- **spelling** - are there any errors within the document?
- **layout** - do the header / footer / logo match with other documents you have received from this company?
- **content** - can you visually see any adjusted numbers or text?
- **consistency** - does this align to the types of documents previously shared by this partner?

If you have any suspicions, then you should reach out to your contact through your secure communication channels. Be careful to use different channels; for example, if the document has been shared by email, you should try to confirm suspicions by phone.

Examples of fake document fraud

This type of fraud can take place on any documents shared between parties. Examples may include, passports, certificates, guarantees, invoices, and manual instructions, however in practice the list may be much larger depending on your business.

Precautions to take:

- Always be cautious when receiving a document required to trigger a business activity.
- Always validate documents that are received - their authenticity is not guaranteed just because they are sent by email or mail.
- Insist on using secure communication channels wherever possible.
- Ensure knowledge is shared within the organization prior to holiday periods.
- In the event of an urgent request, always call the person who made the request back on a known, previously verified phone number.
- Ask employees to limit the level of detail in their social media expressions on the role they occupy within the organization.