Safeguard your business against fraud

Corporate fraud – Invoice 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 fraudpayments@ing.com

Invoice fraud, what is it?

Invoice fraud is manifold. In all cases, the fraudsters will change the banking details of the company which issued the invoice to their own and, as a result, receive the invoiced amounts.

What happens?

1. The criminals intercept the invoice between the time it is posted and its receipt, by hacking the mail accounts used for sending invoices by email, by registering a domain that looks alike the original senders one (so-called domain typo squatting), or by impersonating an existing relation such as a supplier.
2. The fraudsters change the invoice to reflect their own banking details on it. A new invoice is compiled with the new details, with the 'fraudsters' banking details and mentioning a change of bank, etc. Then the invoice is sent again.
3. The invoice is received and paid to the new bank account number. It is highly likely that the following invoices will also be paid to the wrong account until the real issuer of the invoice realises that their invoices have not been paid and contacts the debiting company.

Variants of such fraud

For instance, the debiting company receives an email from what looks like its supplier, stating a change of bank and account number. The message will seem legitimate because it will bear the suppliers' letterhead. In this case, all pending invoices as well as subsequent invoices will be paid to the new account number.

Whatever the scenario, the aim of the criminals is to make a change to what we call the suppliers details (phone number, bank references, email address) in order to steal funds.

Disclaimer

What safeguards to take?

- Validate the invoice: check whether you expected the invoice for this amount and check if the supplier details are unchanged compared to previous payments.
- Inform your customers that if they receive a request to change your details (address, phone number, email address, account number, etc.), they should call you on a previously verified phone number given by you to your customers to check if the requested change is valid. Your customers should not use any phone number indicated on the request itself.
- The same applies to you: if you receive a request to change your supplier's details, you should make a phone call to a previously verified number to check the validity of the requested change. And also in this case you should not use to the number indicated on the request itself.

ING