Safeguard your business against fraud

Corporate fraud – eBanking 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

eBanking fraud, what is it?

eBanking fraud covers all kinds of phishing and malware infections related to the acces of e-banking. E-banking is any form a client can independently execute payments through a website or app, for example Inside Business. Cybercriminals will try to steal money by luring you to give up identification codes and other information to gain access to your accounts. Fraudsters target you in various ways, of which the most important are explained below. Please take your time to inform yourself about the topic as to prevent being tricked.

What happens?

Supposedly, you receive an email from your bank that claims one of the following: the bank is doing a security check, your account will be blocked or that the bank is changing some of its services. The aim is to get you to click on a link that diverts you to a false identification page that looks similar to your online banking.
On that page, you enter your access codes that can be easily retrieved by criminals. With your codes, they have access to your online banking and can execute transactions on your behalf.

Variations of such eBanking fraud

- You receive a call from the fraudster pretending to be a bank employee, and they ask you to perform some sort of security check or 'update', requiring you to generate one or multiple response codes with your smartcard and reader. A real employee will never ask you to do this. The fraudster will use these to access your personal eBanking profile and sign transactions on your behalf. Nor will we ever ask for personal details as id numbers, pincodes etc.
- You receive an SMS which seems to come from ING with a link to a fake ING Website. You click on the link and once you land on the fake website you are asked to fill in codes and personal data. While you are doing this you are called by a fake ING agent on your mobile asking credentials needed for fraudulent enrolment of the fraudsters. Once the fraudsters are enrolled they can take over your account and transfer all of your money out of your account.
- Your computer is infected with malware. Such infections typically occur from opening attachments, links from malicious e-mails or from visiting compromised websites that exploit vulnerabilities in your web browser or operating system. Depending on the type of malware, there are several scenarios that fraudsters use to attack a user, depending on the type of malware. Ultimately, they all lead to the malware trying to create and execute fraudulent payments on your behalf.
- You Google for "login InsideBusiness" (or similar queries) and, is the top result, you get a fraudulent Google Ad leading to a fake ING Wholesale Banking or InsideBusiness website. These fake pages are almost indistinguishable from the real ones. Fraudsters will try to obtain your login credentials through this fake website and use the information you give them to login to the bank's eBanking website and enter and sign transactions on your behalf.
- Breaking into you facilities. Trying to steal card readers and I-Dentity cards hoping to find the PIN code on the with for example a sticky note.

Proper management of online means of payment

Some corporate behaviours can facilitate fraudsters and increase your exposure to fraud:

- Poor management of dual signing: Dual signatures is a means for detecting and preventing fraud. The person who must add the second signature has a second look at the transaction, should not be involved in the transaction itself and can easier detect fraud. Never leave both signatures in the hands of the same person and check what you are signing. Always make sure that first and second signers use different PC's, as this will increase your chance of detecting fraudulent payments created by malware.
- Do not use the autorisation device and PIN of another user as this will cancel out the segregation of duties control. You should only be able to act in accordance with your own permissions.

What safeguards can you take?

- Check that you go to the **correct login page**: https://insidebusiness.ingwb.com/. Save this link in your favorites and preferabvly do not use google to search to find the ING website. If you do make sure to always check if Google Search results and Google Ads lead you **to ING's safe and secure websites: ingwb.com or new.ingwb.com**.
- Besides the URL also **check the padlock** in the address bar of your browser. That means that the connection is secure and you can check that the certificate has been granted to ING Group N.V.
- Keep your PIN, Pasport number/ ID card number and generated security codes secret. Never reveal these secret codes to anyone who asks for them. **ING staff will never ask you for your codes or PIN**. If someone is asking for them, end the conversation and immediately inform your bank about the incident. Never generate a security code when not accessing or using online banking yourself.
- ING will never send you an SMS with a request to follow a link.
- Never store your personal I-Dentity card in a desk or drawer. Keep the card with you so when somebody breaks into your facility they cannot steal the card. And **never ever** store the PIN together with the I-Dentity card.
- **Implement dual signing**. The person who adds the second signature performs an independent review of the transaction and can detect fraud more easily. Never leave both signatures in the hands of the same person and always check what you are signing. Also make sure that 1st and 2nd signers use different PCs as this will increase your chance of detecting fraudulent payments created by malware. Even if your account has been taken over by fraudsters they still cannot execute a payment because they also need the second signature.Do not use the autorisation device and PIN of another user as this will cancel out the segregation of duties control. You should only be able to act in accordance with your own permissions.
- Always **check the details**, i.e. amount, beneficiary name and account numbers of all payments you are about to sign.
- On a periodical basis, at least once every 3 months, check your registered access means for InsideBusiness, and the access means of your colleagues Correct the acces rights if needed to reflect the correct level of access that your employees should have and removes those that are no longer needed or from people that have left your organisation.
- Always close an active web browser session properly by clicking on 'Log out' and never leave your computer unattended when you have an active session. Close the session or lock your computer.
- Check your statements;reconcile them regularly and have your debits and credits regularly reviewed for any abnormalities at least once a week by an independent employee who is not directly involved in the payments process.
- Protect your work environment by reading and applying the information ING has provided with regards to ensuring a safe work environment.

What to do when fraud has occured

- Report fraudulent e-mails and websites to valse-email@ing.nl.
- When you feel you're being targeted by a fraudster, close the active browser session, stop the phone conversation and report fraud to your ING contact. If your ING contact is not available, please call ING Wholesale Banking, Fraud operations: +31 20 584 7840. Outside working hours, please contact fraudpayments@ing.com.