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 phishing and malware infections. It can affect your company or your private life. Whatever the case, cyber criminals will try to steal money by recovering identification codes and electronic signatures from their victim. With these codes, they transfer funds to their accounts and empty your bank accounts instead.

What happens?

1. 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.
2. 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 a fraudster pretending to be a bank employee. He/she asks you to perform some sort of security check or “update”, which means you have to give them the codes with your smartcard and reader. The fraudster will use these to access your personal eBanking profile and sign transactions on your behalf.

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.
- Shared access: Don’t use shared authorisation devices. This will improve security for the company and for the person who will only be able to act in accordance with its permissions.

- 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.
- 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.

  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.

What safeguards can you take?

- Protect your work environment by reading and applying the information ING has provided with regards to ensuring a safe work environment.
- Keep your PIN and generated security codes secret. Never reveal these secret codes to anyone who asks for them, i.e. by phone, in an e-mail, via text message (SMS), WhatsApp message, chat program or face-to-face. ING staff will never ask you for your codes or PIN. If someone is asking for them, end the conversation and inform your bank about the incident.
- Always check if Google Search results and Google Ads lead you to ING's safe and secure websites: ingwb.com or new.ingwb.com.
- Check that you login on the correct login page: https://insidebusiness.ingwb.com/.
- Check the internet address and 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.
- Never generate a security code when not accessing or using online banking yourself.
- Always check the details, i.e. amount, beneficiary name and account numbers of all payments you are about to sign.
- Always close an active web browser session properly by clicking on 'Log out'. Never leave your computer unattended when you have an active session: Close the session or lock your computer.
- Implement dual signing: The person who must add the second signature has an external look at the transaction and can detect fraud more easily. Never leave both signatures in the hands of the same person and check what you are signing. Always make sure that 1st and 2nd signers use different PCs as this will increase your chance of detecting fraudulent payments created by malware.
- On a periodical basis, check your registered access means for InsideBusiness, and the access means of your colleagues.
- Check your statements and reconcile them regularly. Conscious banking is safe banking. And that's how you do it. View your debits and credits regularly at least once a week.
- Report fraudulent e-mails and websites to valse-email@ing.nl.