CEO Fraud

So-called "CEO fraud" is an unscrupulous scam tactic. It involves company employees with direct payment authority receiving an e-mail from one of their superiors asking them to initiate a payment to a certain recipient as soon as possible. In reality though, the sender address is faked, with a fraudster hiding behind it.

The most important points for employees to remember:

- Do not disclose any information if you are contacted in an unusual or dubious way, and do not follow any instructions, even if you are put under pressure.
- Before executing any such payment requests, immediately ask your superior via another channel (in person or by telephone) to confirm them.
- Look out for any missing or incorrect security elements such as e-mail signatures (https://www.ebas.ch/en/e-mail-signatur-outlook/).

The most important points for companies to remember:

- Ensure your employees are aware of this type of fraud.
- Check what kind of information is available about your company online, and limit this where possible and expedient.
- Define and implement a payment release process involving double checks and joint signatures.
- You should also report any such attempts at fraud to the police.
- Check that advanced security elements such as e-mail signatures are implemented in critical business processes (payment process).

Secure employee behaviour

If one of your supervisors sends you an e-mail asking you to initiate an immediate payment which has not been discussed in advance or was previously unknown to you, you should be extra careful. In such unusual cases, it is advisable to clarify the legitimacy of such an order more thoroughly, for instance by checking any security elements like e-mail signatures (digital signatures) are in place. **You should certainly always contact that supervisor directly (in person or at least via telephone) and confirm whether this payment is actually to go ahead.**

Take precautions as a company

Sensitising employees

Technical means only help to curb the distribution of such fraudulent e-mails to a certain extent, but can never completely prevent it. Fraudsters are constantly changing their addresses, concealing their identify and origin this way. In addition, they also sometimes manage to abuse a superior's authentic e-mail account for their purposes.

The most important prevention measure is therefore sensitising your employees working in all departments

most susceptible to this kind of fraud, for instance in your accounts department.

Online information
To initiate a "CEO fraud", the first thing an attacker needs is information about a company and its employees. A company website or the trade register often provide sufficient information of this kind. In addition, social networks (such as LinkedIn (https://www.ebas.ch/en/linkedin-settings/) or Xing) are of interest to fraudsters, since they contain information about business relations or employee identity and roles. You should therefore check what kind of information is available about your company online, and limit this where possible and expedient.

Payment release process
The actual fraud involves the remittance of a payment. This usually has a foreign bank account as the recipient. From there, the funds are then promptly transferred to yet other accounts. To prevent such incorrect payments, it is advisable to establish a strict payment release process complete with checkpoints - with the best method being a system of double checks and joint signatures. This way, there is a considerably higher chance of one of the two people releasing a payment recognising a fraud for what it is and thus preventing it.

Using e-mail signatures
"CEO fraud" manipulates the payment process by faking a legitimate sender of a payment order (so-called e-mail spoofing).

The simplest variation of this is to fake the e-mail sender's address. An e-mail signature (digital signature), which can only be inserted correctly by an authentic sender, provides good protection against this. However, this kind of procedure is relatively difficult to implement and also makes it necessary for the recipient to properly check this signature.

More serious is the abuse of an authentic (hacked) e-mail account of the sender, for instance in consequence of a phishing attack carried out beforehand. This even enables fraudsters to abuse the e-mail signature feature. In such cases, the only remedy is a strict payment release process, and to sensitise all people involved.

With the "CEO fraud" scam (also called Supervisor fraud), attackers pretend to be a company's CEO (company head) and ask employees with payment authority to initiate a remittance of a large sum of money.

"CEO" stands for Chief Executive Officer, "fraud" is self-explanatory here.