Quick guideline

# CEO fraud

Anti Fraud Management

Bundesverband

An employee receives a perfectly authentic e-mail from a management member. The big deal in China that has been discussed in the company for a while is finally approaching. In order to close the deal, USD 750,000 need to be transferred to a bank in Shanghai. However, the transaction is to be treated confidential. The employee knows that the sender of the e-mail is currently in China and hard to contact. The transfer is authorized – and the money is lost.

The sender of the e-mail was actually a criminal who had done some thorough research on the company beforehand. A so-called CEO fraud is hard to detect, but easy to counter – just verify the information!

## CEO fraud – characteristics

- Sender is often an alleged board/management member
- Sender may be known or unknown
- Existing financial flows are to be rerouted
- New funds are to be transferred to a hitherto unknown account
- Affected amounts may be small
- Sender demands confidentiality
- Sender often pushes for fast payment

## A simple countermeasure: verify their identity!

- Examine the e-mail address! In many cases, the e-mail address reveals that, while the sender is allegedly a member of the upper management, they are using a “fake address”.
- Verify the sender‘s identity: Search the intranet for the person‘s official contact details and call back the sender using this official data.
- Do not let the sender pressure you!
  If you are suspicious, contact your manager and the security department.
- Obtain additional information from the competent security authorities.
  They will normally provide additional warnings.
- Share this new security information with your company, e.g. via the intranet.
- Raise awareness: Sensitize the departments within your company that may authorize payments (e.g. finance department, CFO)

## Examples

### Case 1

You receive a call or an e-mail from a person you know (allegedly a member of the board/management), instructing you to transfer money or to provide information.

### Recommendation

Call back! Find the official contact details of the person in the intranet (do not use the contact details provided in the e-mail signature!) and verify that the instruction was actually issued by that person. When in doubt, contact the board/management member usually responsible for authorizing payments.

### Case 2

You receive an e-mail from a management member that is personally known to you, demanding an urgent money transfer to a specific account or the modification of a target account.

### Recommendation

Call back! Verify that the e-mail was actually sent by that person.

### Case 3

The e-mail calling for a money transfer also contains the instruction to maintain secrecy.
The sender states that they are difficult to reach via telephone, or only via a different number.

### Recommendation

Call the official number you know! If you are unable to contact the desired person, inform your manager or another member of the management.

### Case 4

A new money transfer is to be authorized on very short notice, practically excluding any verification.

### Recommendation

Especially in such cases, verify the information!
Make sure that the transfer is legitimate.

ASW Bundesverband

**Published by:** ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e. V. | **Updated:** June 2016 | **Contact:** info@asw-bundesverband.de

ASW Bundesverband endeavours to provide correct and updated information.
However, we cannot provide any guarantee regarding the accuracy of the provided information and we do not assume any liability for direct or indirect damages resulting from the use of such information.