Business Email Crime & Social Engineering

Payments Fraud Prevention, Frankfurt/Main

Cyber crime against companies starts directly with employees

Why hackers tend to target employees (rather than managers):

- Different products for electronic banking
- Nationally bigger differences in the technologies and authorisation media used
- The payment processing products used in Germany have a high level of technical security.

Conclusion

- Fraud scenarios practised abroad became widespread in the German-speaking world in 2015.
- Fraudsters target their attacks at employees within a company to ...

01 Extortion

… ultimately extort them or the company.

02 Payments

… get them to process payments that appear to be legal.

03 Access

… gain access to the employee's work computer to process the payment themselves, e.g. via remote access.

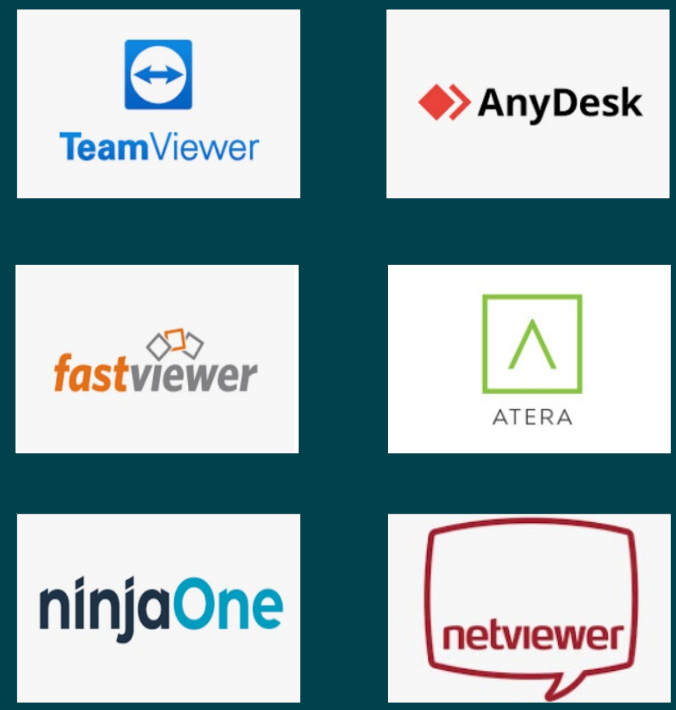
Fraud scenarios

Agenda

Fraud scenario: remote access tool

Fraud with legitimate remote maintenance software

- In retail banking, fraud is often committed using a (purported) Microsoft technician call.
- For companies, information about the firm is gathered in advance to prepare.
- Later someone claiming to be a bank employee calls the employee at the company. Under a pretence, the employee is urged to accept technical support (for example) for a necessary update of the payments system.
- The employee installs a remote access tool (using normally legitimate support software) as instructed by the caller and the fraudster uses the employee to gain access to their work computer.
- The employee is instructed to enter credentials into special and/or unusual fields. That enables the fraudster to read passwords. The access that has been gained and the credentials are used to authorise payments.
- Later, online banking appears to be unavailable because a manual update is being run. In reality, the credentials have been changed by the fraudster in order to take control of your account away from you.

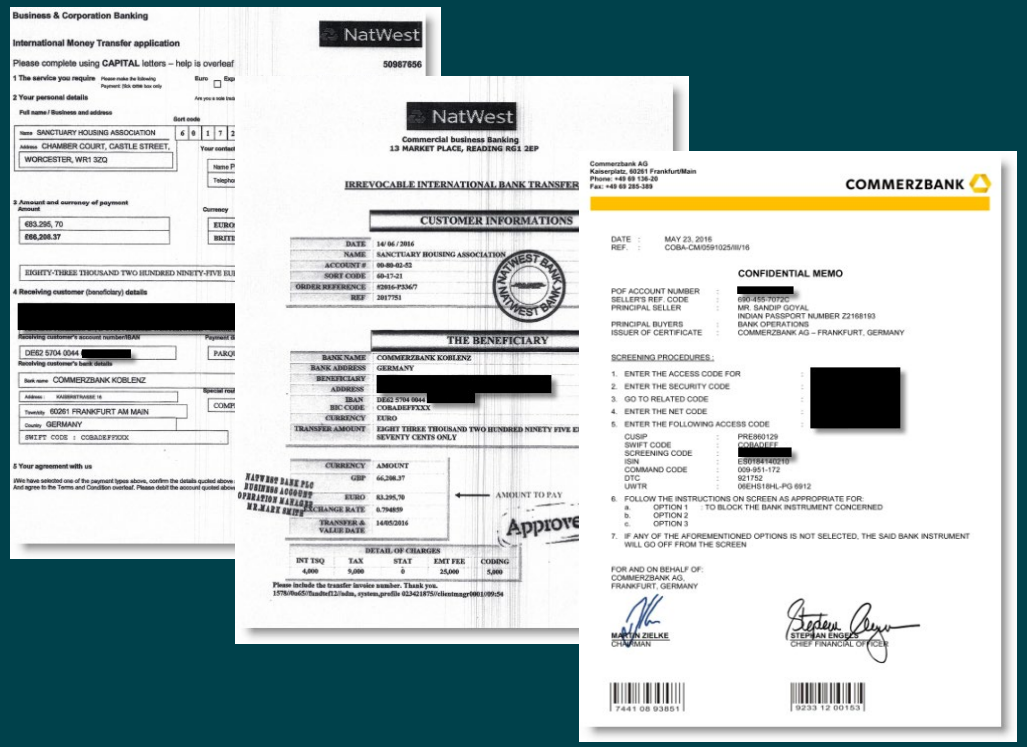


TIP: If you have requested technical support and you receive a call from the person you expected, it is unlikely to be fraud. If someone pushes software on you and tries to get you to believe there are problems you do not see, it is probably fraud.

Fraud scenario: fake payment

A demand is made for goods to be delivered, but the payment is faked.

- Arrangements are made for a transaction and a partial payment or advance payment is agreed.
- The goods are produced and prepared for the client. The deposit is made as it should be.
- Shortly before the delivery date, the recipient sends an allegedly genuine proof of payment, account statement or even a supposed SWIFT confirmation from their bank saying payment has been made.
- The goods are sent.
- Later it turns out to have been a front company (shell company).
- The payment confirmations were fabricated. The money never arrives. The ordering party's alleged account usually does not even exist.

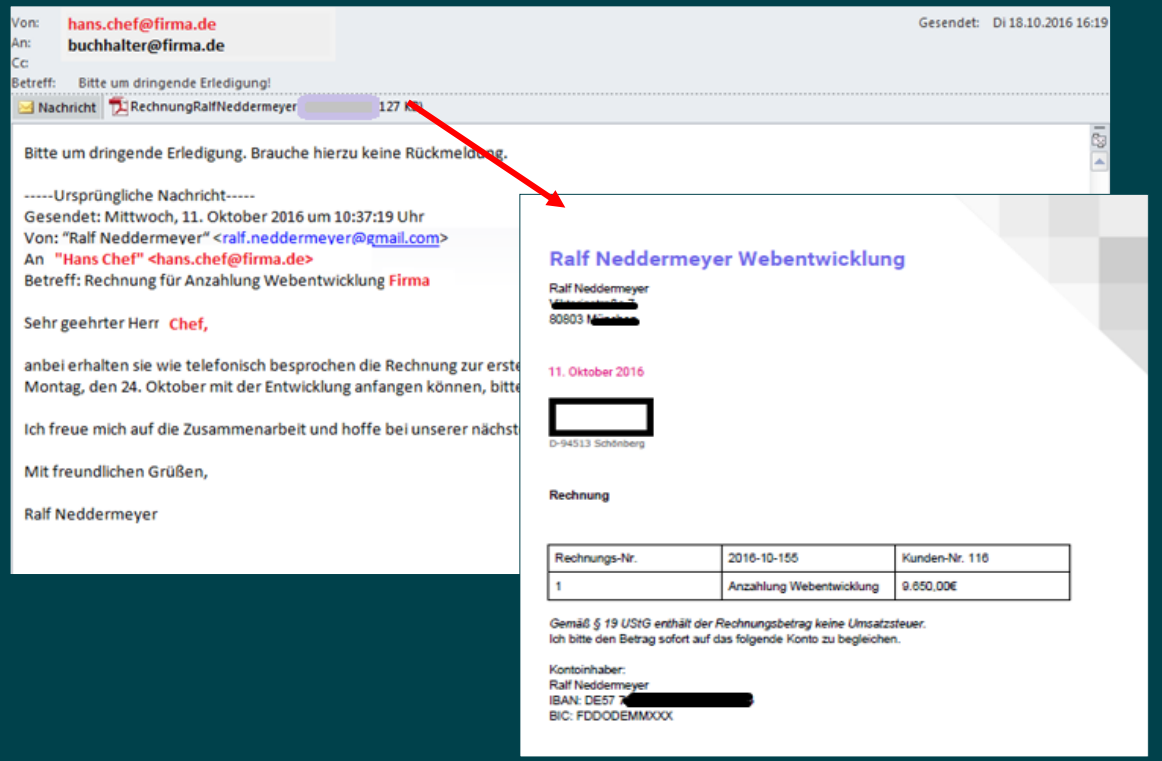


TIP: A transfer has a legal form that has a discharging effect when the amount is credited to the recipient's account. So check the alleged proof of payment for clues that it might be fake and put safeguards in place to protect international transactions with new business partners. Do internet research.

Fraud scenario: invoice fraud

A new take on invoice fraud is when an alleged boss wants the transfer or a lawyer insists on bills being paid.

- In one version, a final warning is sent to an accountant. A little later a lawyer for the company calls and requests payment. If requested, bogus invoices and orders are sent straight away.
- In another version, an accountant receives an alleged email forwarded from their boss requesting payment. An invoice and invented order history are attached.
- In current versions, the employee only receives a question from the manager about how much money is left in the account and whether an international transfer can still be executed today. Instructions are issued based on the response.
- Damages in individual cases run between EUR 10,000 and EUR 180,000.
- Pay attention to the legitimacy of the sender. The inbox overview does NOT list the sender.

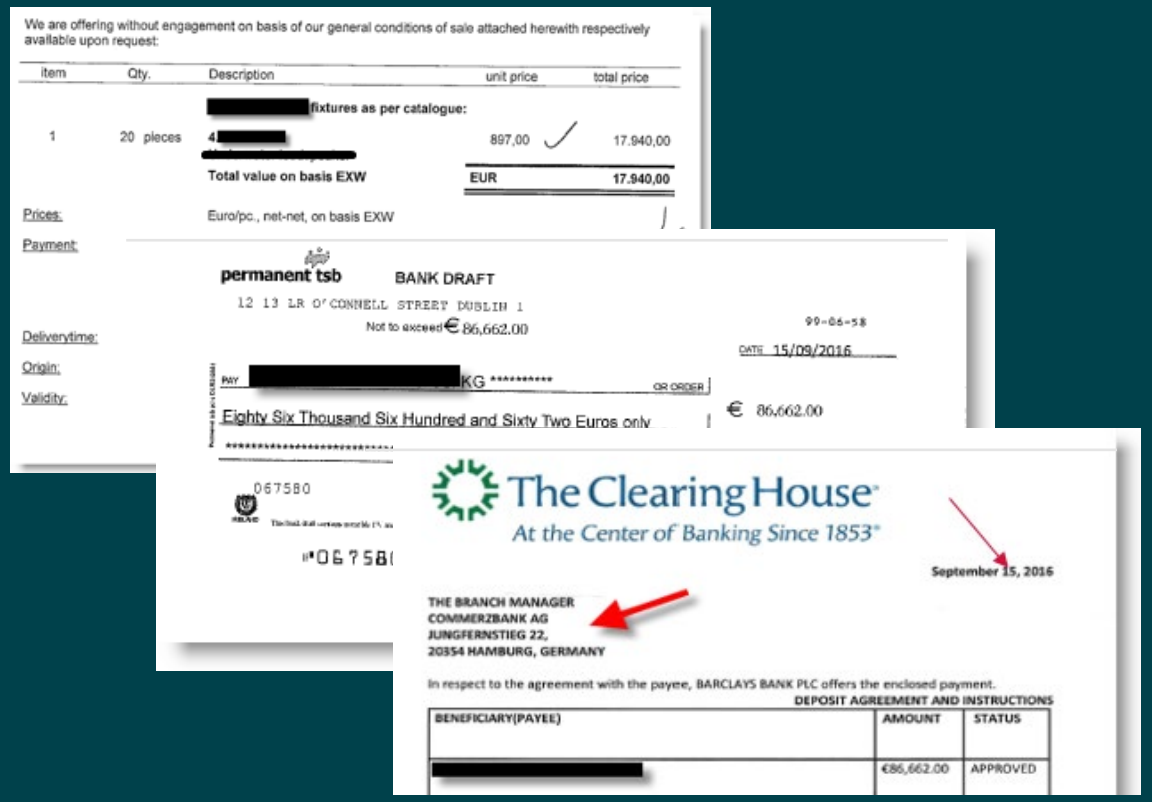


TIP: Educate your employees about this type of fraud. Invoices should not be paid without the proper process or order. Use the Outlook functions that signal whether a recipient is within your organisation or outside of it.

Fraud scenario: cheque overpayment

The cheque bounces. Your reverse transfer cannot be undone.

- **Traditional form:** Payment by cheque is requested when an order or booking is placed. The cheque is then issued in excess of the amount needed and the person requests that the "accidental" overpayment is transferred back to them.
- **New form:** Your company accepts an order. You request payment by transfer and provide your IBAN. That gives the fraudster your bank's address.
- An overpayment by cheque is sent directly to your bank with a fraudulent letter. The letter requests that the amount be credited to your account.
- Once the money is paid in, you have unexplained income.
- A little later, the fraudster's email arrives saying that their accounting department accidentally mixed up two transactions. They "transferred" you too much money, the amount of a different invoice.
- The fraudster knows that you only know the amount credited but never held the cheque in your hands. He requests that the difference be transferred back. The cheque is bogus and "bounces".

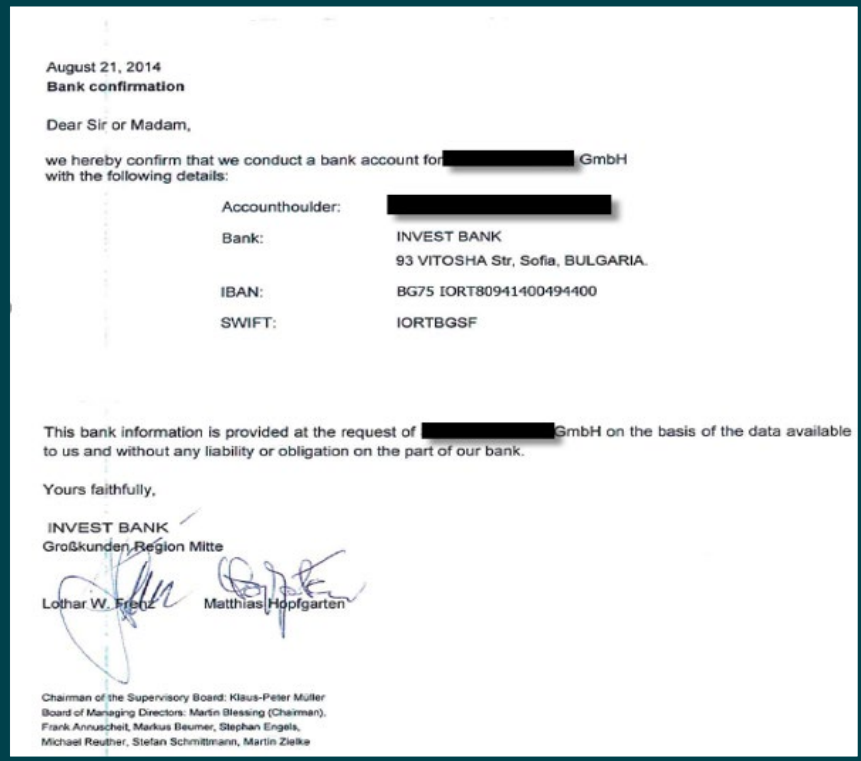


TIP: Check carefully if a credit is a cheque deposit. Depending on the country, a cheque can be cancelled for ten days at a minimum, sometimes months. We call you before depositing cheques from third parties. If you did not request a cheque deposit, contact your bank immediately.

Fraud scenario: payment diversion

When bank account details suddenly change

- It appears that your business partner is correcting the bank account details.
- It may be done directly via a genuine email in an invoice if your business partner's email system has been compromised.
- Falsified changes to bank account details in the name of an employee to redirect salary payments may also occur.
- Wrong bank account details may be received by email, fax or letter.
- If the change is made without reference to an invoice, it usually happens with companies when goods are delivered or services provided under framework agreements (mining, travel companies, chemicals, automotive suppliers, etc.).
- The scam is noticed only when the business partner issues a payment reminder. Time is often lost requesting that the fraudulent transfer be investigated.



August 21, 2014
Bank confirmation

Dear Sir or Madam,

we hereby confirm that we conduct a bank account for [redacted] GmbH with the following details:

Accounthoulder:	[redacted]
Bank:	INVEST BANK 93 VITOSHA Str, Sofia, BULGARIA.
IBAN:	BG75 IORT80941400494400
SWIFT:	IORTBGSF

This bank information is provided at the request of [redacted] GmbH on the basis of the data available to us and without any liability or obligation on the part of our bank.

Yours faithfully,

INVEST BANK
Großkunden Region Mitte

Lothar W. Frenz Matthias Hopfgarten

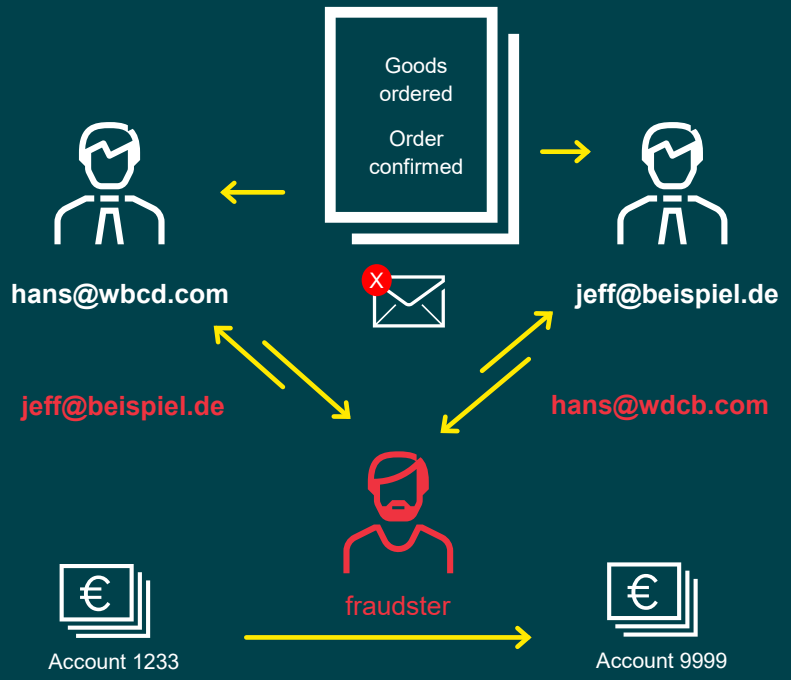
Chairman of the Supervisory Board: Klaus-Peter Müller
Board of Managing Directors: Martin Blessing (Chairman),
Frank Annuscheit, Markus Beumer, Stephan Engels,
Michael Reuther, Stefan Schmittmann, Martin Zielke

TIP: Ensure your email communications are secure. Unencrypted email is like a postcard. Protect your master data, such as bank accounts and your business partners' delivery addresses. Require the people you are contracting with to do the same. Question any change, preferably using a different "channel" (e.g. call).

Fraud scenario: man in the middle (PD)

Somewhere in one of the email replies, the sender's name changes suddenly by only one or two characters.

- Business partners are arranging a deal and even ask each other some personal questions at the beginning. Then the order is made.
- You do not notice that other similar looking email addresses creep in as you communicate over time.
- Because the content is practically the same as the original and the chain of messages is there, no alarms are raised when the bank account details are changed when the invoice is generated.
- The bank account details in the invoice have been manipulated. The invoice is not unexpected, however, and had been approved.
- The scam is only noticed when your business partner sends a payment reminder or when the goods do not get to the party who paid for them.
- Time is often lost requesting that the fraudulent transfer be investigated.



TIP: Sichern Ensure your email communications are secure. Unencrypted email is like a postcard. Protect your master data such as bank accounts and your business partners' delivery addresses. Require the people you are contracting with to do the same. Question any change, preferably using a different "channel" (e.g. call).

Fraud scenario: CEO fraud (aka "boss scam")

The individual employee becomes the fraudster's drone. Trust in the principal bank is exploited.

- Your company may be spied on months before the scam sometimes. Data is gathered from the internet, public registers, social media used for professional purposes and sometimes seemingly irrelevant calls.
- The employee receives an email or a call, allegedly from their boss.
  They are entrusted with a confidential financial matter and are told to contact an advisor/lawyer at a reputable law firm/consultancy.
- The confidentiality is repeatedly emphasised. Outstanding information is requested: accounts, balances, authorised parties.
- The employee later receives a transfer order that has already been signed.
- The employee makes the transfer, other "payments" are required. The fraudster calls until the scam is noticed or the money runs out.

Von: **Hans Chef:** hans.chef@firma.de,
<cc.bafin@munich.com>
Gesendet: Montag, 15. Februar 2016 11:13
An: [redacted]
Cc: cc.bafin@munich.com
Betreff: vertraulich

Sehr geehrte Frau [redacted]

zurzeit bereiten wir die Übernahme eines Unternehmens vor, dies betrifft insbesondere die erforderlichen finanziellen Transaktionen.

Die Angelegenheit muss absolut vertraulich behandelt werden. Niemand sonst, auch nicht innerhalb unseres Hauses, wird zurzeit darüber informiert.

Die öffentliche Bekanntmachung des Übernahmeangebots erfolgt in Kürze.

Aufgrund Ihrer Diskretion und bisher einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen.

Ich bitte Sie, umgehend Herr Dr. Mueller von der Kanzlei KPMG (tomas.mueller@consultant.com) zunächst unsere Bankverbindung für die weitere Bearbeitung zu übermitteln.

Da die gesamte Transaktion absolut vertraulich behandelt werden muss bitte ich Sie, den Stand der Transaktion nur mit mir ausnahmslos per E-Mail abzustimmen.

Weiter bitte ich Sie, mich in dieser Angelegenheit weder persönlich noch telefonisch zu kontaktieren. Jede Erörterung der geplanten Übernahme erfolgt ausnahmslos per E-Mail an Sie oder mich, auch um eine ausreichende Dokumentation gemäß den BAFin Richtlinien sicherzustellen.

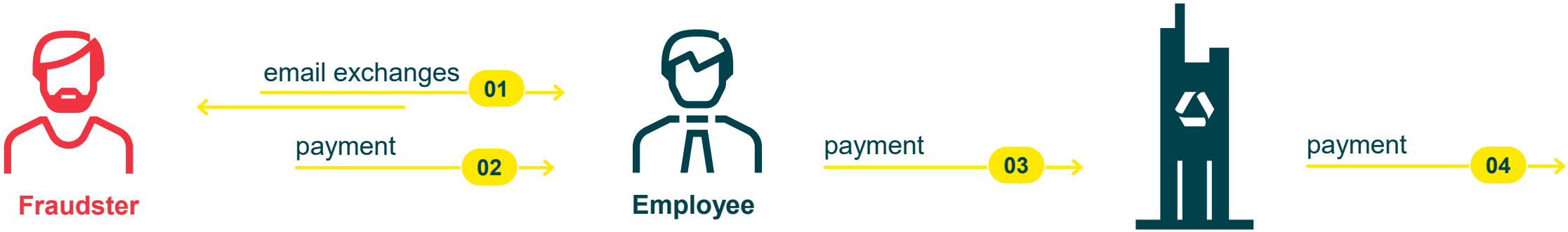
Ich zähle auf Ihre Diskretion und bedanke mich schon jetzt für Ihre Mitarbeit.

Mit freundlichen Grüßen

Geschäftsführer

TIP: Always also call us if there is ever a CEO fraud attempt, even if the employee spots the email. Educate people about this sort of fraud. Use the Outlook functions that show whether a recipient is within your organisation.

Fraud scenario: CEO fraud



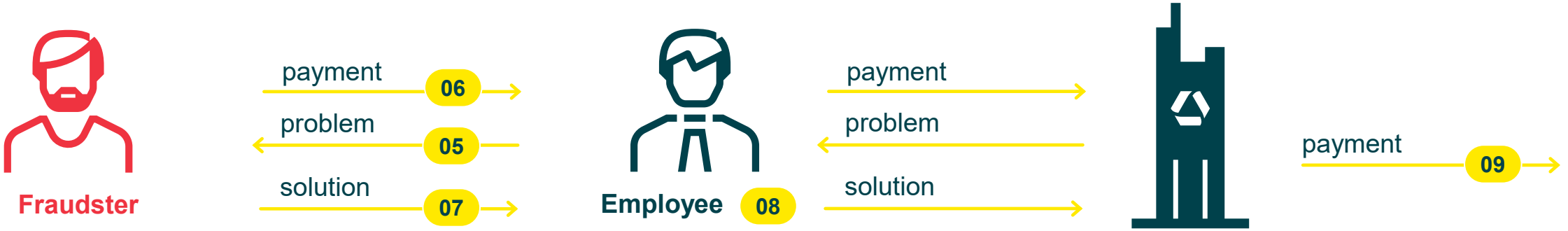
01 The alleged boss entrusts the employee in strictest confidence with a task. They should provide a third party (lawyer, consultancy, law firm) with all the necessary information by email.

02 The employee is then contacted by the third party, skilfully assured and manipulated. The goal is to get further information (limits, authorisations, necessary signatures).

03 The employee is instructed to make payment; naturally with signatures that have already been provided that they had previously said were required (distributed signature). Throughout they are adeptly involved in the email exchange between the alleged boss and the third party.

04 The employee that we as the bank know and trust instructs us to make the payment with the requested urgency. Follow-up questions are generally not answered for confidentiality reasons.

Fraud scenario: CEO fraud



05 Problems are resolved with the alleged boss. Unauthorised signatures should now be authorised using the Commercial Register (for example).

06 They work with fake documents, identifications, certifications and BaFin documentation. The employee within the company is used to pressure the bank. The payment is supposedly urgent after all.

07 Requested assurances and confirmations are provided.

08 If the balance in the account is not sufficient to make the payment, the employee is sent to the bank to ask for an overdraft. A balancing payment is promised for the next day, and with money supposedly from the holding company or a subsidiary. If those do not exist, the fraudster is content to take smaller amounts too.

09 When the bank asks whether it could be fraudulent, the answer is no: "The payment is OK."

Even any questions from the internal compliance department within the company are brushed away with reference to the requested confidentiality.

Fraud scenario: extortion

Do you gain anything from disclosing the information?

Rule number 1: If something is free, you are paying with your data.

- Possible scenario: An employee has information on Xing, for example, and someone using a false identity posing as a headhunter or consultant requests that they be added as a contact. By confirming the request, the employee discloses their network and data, assuming that they had not already made them available for all to see because of inadequate privacy settings.
- If the employee uses the same name in the social media they use privately, if they disclose private information there or accept friend requests from people they do not know personally and if they are possibly connected to their own children who in turn post where they play sports, then there is potential for blackmail.
- Other versions: spam blackmail emails claim to have accessed your laptop camera and threaten to release the recorded images if you do not...
- New social media threat: sextortion

Social Media

XING

LinkedIn

Facebook

Twitter

Fraud scenario: extortion trojans

The client is attacked using malware or a hack. The company's files are copied and encrypted.

- Prevention is the only cost-effective course. Invest in your IT security and IT surveillance!
- Sudden disaster scenario. The only things that help when a company is encrypted are Offsite-backups and offsite emergency plans.
- No more backups? The damage is often greater than the ransom. Pay? Will you get a key? Will the data be saved?
- Report the issue to your insurer if you have cyber insurance.
- The largest ransom demanded we are aware of in Bitcoin: EUR 240 million
- **We advise against paying!**
- Do not forget the GDPR! Anyone failing to report a relevant incident within 72 hours can be fined.
- We strongly recommend getting the police involved (central cyber crime desk of the criminal police force in each Federal state).
- Leave the work to IT forensics specialists. Internal IT departments often do not have the necessary skills and/or capacities to deal with the situation. Decryption after the fact is almost never possible.

Videos

01 Secuso.org on YouTube (German)

This video is about pitfalls in handling emails. How do I distinguish between real and fake links and what do I need to look for?
Secuso.org originated at Darmstadt University and has a number of such videos on the internet.
https://youtu.be/4xIU1lPJs_4

02 Fusion.net on YouTube (English)

This video shows a social hacker a reporter has asked to demonstrate how easy social hacking is.
She is actually only supposed to find the reporter's email address but by the end she takes control of his entire mobile phone account using a simple trick that the hotline worker she phones is very happy to help with.
https://youtu.be/lc7scxvKQOo

03 Gravoc on YouTube (English)

An animated clip shows the typical key points to know in order to avoid social engineering. The attack usually comes via channels that people are not initially paying attention to.
https://youtu.be/Vo1urF6S4u0


COMMERZBANK