

# FRAUD SCAMS TARGETING EMPLOYEES HOW TO PROTECT YOURSELF ?



## KEY TARGETS

Mid-level employees in financial or procurement services

## HIGHLY ATTRACTIVE CRIME

large profits and low risk of detection

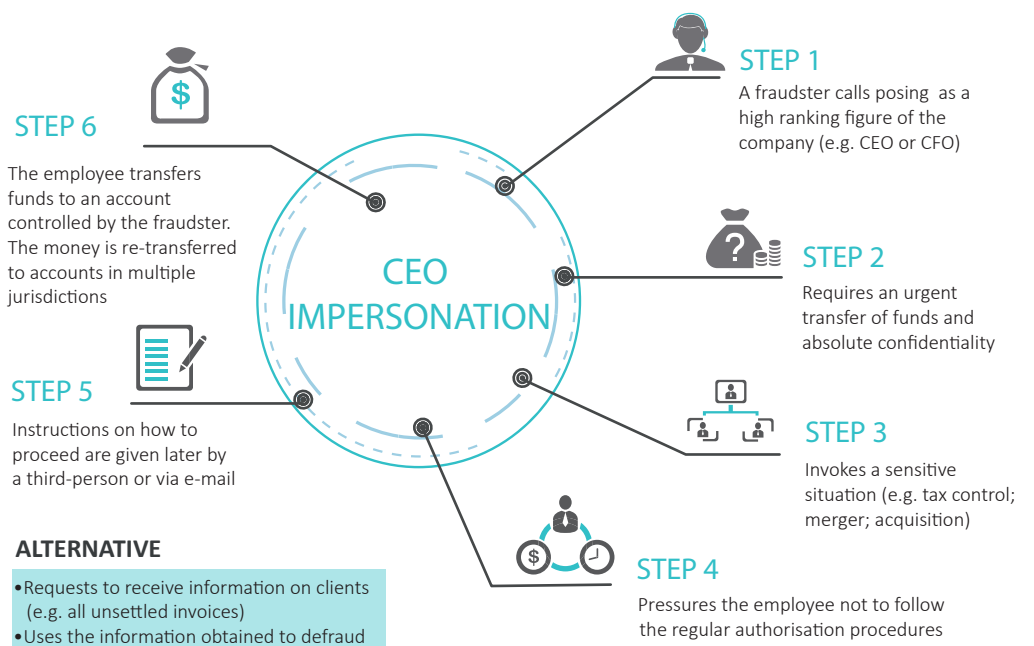
High financial impact for targeted companies:  
**LOSSES UP TO SEVERAL MILLION EUROS**

## DIRECT HUMAN COSTS

shame; sanctions; loss of employment

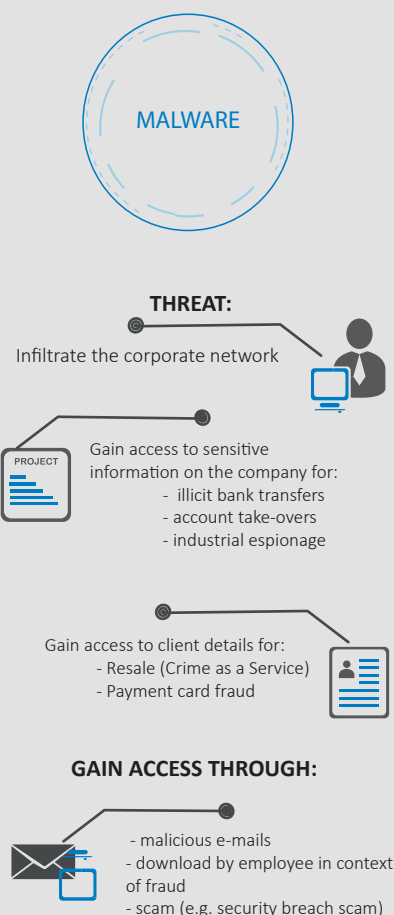
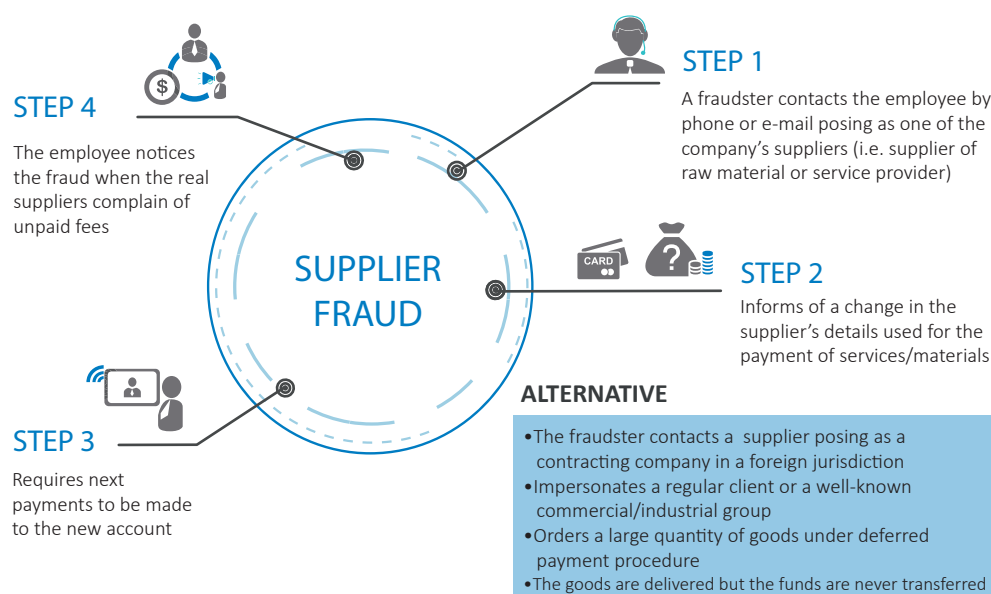
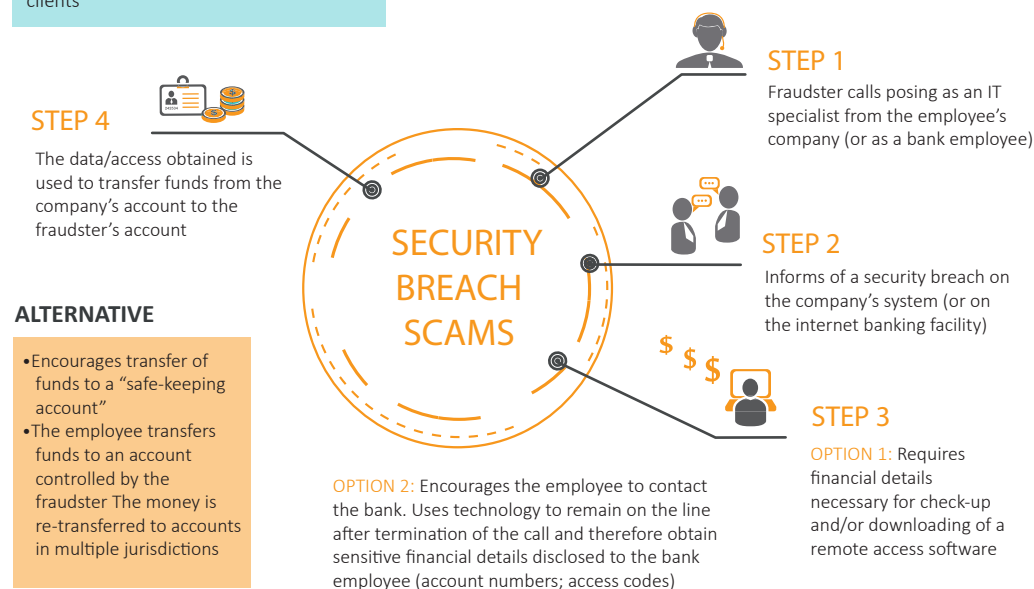


## KNOW THE SCAMS



### HOW DO FRAUDSTERS CONCEAL THEIR IDENTITY?

- Use forged documents with legitimate company logo/signatures obtained online
- Use copycat e-mail addresses
- Disguise the origin of the call through applications faking the caller's identity (display the number of the service/individual they impersonate)
- Use VOIP and proxy servers to lower the risks of detection
- Use the services of illicit call centres based outside the EU



## KNOW THE SIGNS



- Unsolicited call/e-mail requesting information on internal procedures for payment or procurement
- Unsolicited call/e-mail requesting financial information (account numbers, access codes)
- Feeling of emergency
- Pressure

### CEO IMPERSONATION

- Direct contact by a senior official you are normally not in contact with
- Unusual request in contradiction with internal procedures
- Request for absolute confidentiality
- Threats or unusual flattery/promises of reward

### SECURITY BREACH SCAM

- Use of particularly alarming tone by an IT/security officer
- Request to download external software (e.g. remote access software)
- Offer of a safe-keeping account

### SUPPLIER FRAUD

- Sudden change in contact/payment details of an international supplier (would normally be announced a few weeks/months in advance)
- Change occurring shortly after a significant order was passed or shortly before a deadline for payment

### MALWARE

- Unsolicited e-mails with generic greetings
- Unsolicited e-mail containing suspicious links/URLs



## KNOW HOW TO REACT



- Be AWARE of the risks and spread the information within your company.
- Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- Avoid sharing sensitive information on the company's hierarchy, security or procedures.
- Never open suspicious links or attachments received by e-mail. Be particularly careful when checking your personal mail boxes on the company's computers.
- If you receive a suspicious e-mail or call, always inform your IT department; they are the ones in charge of such issues. They can check the content of suspicious mail and block the sender if necessary.
- Always carefully check e-mail addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat e-mails where only one character differs from the original.
- If you receive a call/email alerting you of a security breach, do not provide information right away or proceed with a transfer. Always start by calling the person back using a phone number found in your own records or on the official website of the company; do not use the number provided to you in the mail or by the caller. If you were contacted by phone, call back using another phone (fraudsters use technology to remain online after you hang up).
- In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
- Consider assigning responsibility to an employee whom others can consult in case of doubt.
- If a supplier informs you of a change in payment details, always contact him to confirm the new information. Keep in mind that the e-mail/phone number provided on the invoice might have been modified.
- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.