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

EUROPOL

CEO IMPERSONATION

STEP 1
A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)

STEP 2
Requires an urgent transfer of funds and absolute confidentiality

STEP 3
Invokes a sensitive situation (e.g. tax control; merger; acquisition)

STEP 4
Pressures the employee not to follow the regular authorisation procedures

STEP 5
Instructions on how to proceed are given later by a third-person or via e-mail

STEP 6
The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions

ALTERNATIVE
- Requests to receive information on clients (e.g. all unsettled invoices)
- Uses the information obtained to defraud clients

SECURITY BREACH SCAMS

STEP 1
Fraudster calls posing as an IT specialist from the employee's company (or as a bank employee)

STEP 2
Informs of a security breach on the company's system (or on the internet banking facility)

STEP 3
OPTION 1: Requires financial details necessary for check-up and/or downloading of a remote access software

OPTION 2: Encourages the employee to contact the bank. Uses technology to remain on the line after termination of the call and therefore obtain sensitive financial details disclosed to the bank employee (account numbers; access codes)

STEP 4
The data/access obtained is used to transfer funds from the company's account to the fraudster's account

ALTERNATIVE
- Encourages transfer of funds to a "safe-keeping account"
- The employee transfers funds to an account controlled by the fraudster The money is re-transferred to accounts in multiple jurisdictions

SUPPLIER FRAUD

STEP 1
A fraudster contacts the employee by phone or e-mail posing as one of the company's suppliers (i.e. supplier of raw material or service provider)

STEP 2
Informs of a change in the supplier's details used for the payment of services/materials

STEP 3
Requires next payments to be made to the new account

STEP 4
The employee notices the fraud when the real suppliers complain of unpaid fees

ALTERNATIVE
- The fraudster contacts a supplier posing as a contracting company in a foreign jurisdiction
- Impersonates a regular client or a well-known commercial/industrial group
- Orders a large quantity of goods under deferred payment procedure
- The goods are delivered but the funds are never transferred

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

MALWARE

THREAT:
Infiltrate the corporate network

Gain access to sensitive information on the company for:
- illicit bank transfers
- account take-overs
- industrial espionage

Gain access to client details for:
- Resale (Crime as a Service)
- Payment card fraud

GAIN ACCESS THROUGH:
- malicious e-mails
- download by employee in context of fraud
- scam (e.g. security breach scam)

KNOW THE SIGNS

EUROPOL

- 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

EUROPOL

- 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.