How to avoid corporate fraud?

The number of sophisticated digital fraud cases resulting in financial losses for companies has been on the rise. Anyone can be a victim. Learn more about how to spot these situations in your company and find tips on how to avoid them.

Authorised fraud is a well-known method of digital attacks in the corporate environment, where the victim's corporate payments are being manipulated. The perpetrators use a variety of tactics, including:

1. Invoice payment fraud

This type of fraudulent activity involves the **attacker acting like a former or current supplier**.

The invoice from the attacker **looks identical to an actual invoice** (logo, address, company ID), but the **payment details are altered** (IBAN). This can often be overlooked. The attacker assumes employee will not verify the payment details, as this is a long-standing relationship.

Manipulative techniques are also used, such as insisting on payment that's allegedly overdue or direct notification of a change in payment details. In such cases, **it's necessary to verify any changes through contact persons other than the sender of the e-mail**.

2. CEO fraud

CEO fraud involves urgent payments to fraudulent accounts where **the attacker poses as the supervisor of the e-mail recipient**. The perpetrator poses as the company's CEO or CFO and uses **authority for manipulation**.

It can be a **written, phone or manipulated video call communication**. The perpetrator can convincingly **mimic the identity of a real person** thanks to advanced techniques. A phone number can often be **"spoofed"**, which means that it's pretending to be a real person or a company (for example, the name of a supervisor or the name of the company is displayed on the screen).

In such cases, it's also **necessary to ensure multi-level verification of the request** or **use other contact** than the sender/caller for verification.

Methods of fraudulent communication:

Methods of fraudulent communication is a type of electronic communication which can be sent from a real e-mail address because it's been attacked by malware. The attacker may also use an e-mail address similar to the e-mail of your supplier (for example, they change one letter: *instead of 'emerald' they use 'ernerald' or add an 's' at the end – 'holdings.com' instead of 'holding.com')*.

TATRA BANKA
Member of RBI Group

What is a malware?

Malicious software that aims to damage or abuse devices, networks or a service. It may also include **phishing attacks to access the victim's e-mail account** or operating system. Attackers can monitor communications and identify payment opportunities to target fraud once they gain access.

How does malware spread?

Malware spreads mainly through e-mail attachments, malware ads on popular websites (malvertising) or fake software – but also through compromised USBs, apps or text messages.

The difference between a malware and phishing attack:

Malware, as opposed to a phishing attack, is a **fraudulent redirection of payments aimed at individuals** or a couple of employees (a single division). It doesn't target the whole company. This focus on individuals may increase the success rate of malware. If an employee makes a payment according to the instructions, no other employees are affected, and they won't notice or report the fraudulent activity.

How to avoid authorised fraud:

1. Education

An efficient method for authorised fraud prevention is **regular education of employees**. Employees can prevent fraudulent attacks at companies thanks to sufficient awareness of fraudulent communication methods.

2. Direct verification

You always need to **adequately verify any change related to payment through a communication channel** other than the one from which the request was sent. Links or other contact details in the e-mail or letter with the request for change can be fraudulent. These are **certainly not advisable to use**.

3. Multi-level verification

Accountants and employees with access to payments should perform **multi-level verification**:

- Verification of business partner via official corporate system.
- Verification of the e-mail from which the request was sent.
- Verification of non-standard communication method through a channel other than the incoming communication (e.g. phone verification).

4. Report authorised fraud ASAP

Investigating such criminal activity is extremely difficult because funds are transferred quickly. The likelihood of funds being returned to the victims is low, especially if the incident is reported with a delay. That's why it's important to educate employees regularly and ensure preventive checks of payments, which can help you avoid fraudulent behaviour.

For more information,
please visit https://www.tatrabanka.sk/predigitalnubezpecnost/en/security-and-companies/

TATRA BANKA
Member of RBI Group