WRITTEN BY

ANGELIKA KODHAJOVA
Data protection & Security Specialist
DEUTSCHE TELEKOM SERVICES EUROPE SLOVAKIA s.r.o.

CEO FRAUDS USING AI

The fraudsters are increasingly using new technologies such as deepfakes to scam victims. More than ever, we need to better understand fraud threats and improve our personal level of defense. According to Metro Atlanta CEO the number of deepfakes in the crypto industry increased in 2023 by 128% compared to 2022.

CEO Fraud is a cybercrime where cybercriminals impersonate executives or spoof company email accounts, which is then called spear phishing. They primarily target high-level executives, HR personnel, or employees authorized for wire transfers, aiming to deceive them into making unauthorized transfers or disclosing sensitive information. Indicators of CEO fraud include suspicious links or attachments, misspellings, requests for sensitive data, and urgent requests.

WHY IS CEO FRAUD SO ATTRACTIVE?

Criminals are constantly monitoring how new technologies can be exploited and incorporated into their toolkits to attack account holders. Let's have a look at two technologies that can enhance frauds.

The common indicators of CEO fraud have slightly changed since AI entered the scene. There is flawless grammar in any language. When spoofing the emails, the AI convincingly refers to the context of the previous communication between the fraudulent executives and their business partners which significantly increases the credibility of these emails.

The increased adoption of Fast Payments Systems (FPS) has led to a rise in frauds as it helped to extend the tools portfolio used by attackers. The speed at which funds become available to the recipient and the ability to send a large amount of money in a single transaction is often what makes fast payments attractive for fraudsters. By the time a transaction is deemed to have been fraudulent, the illegally obtained funds may already be gone. This can make lost funds very hard or impossible to be reversed.

The bank can call you or block your credit card if it was used for the first time abroad, to verify with you if there has been any abuse. But when you transfer several million euros in one payment to any of the third world countries, despite the fact that your money transfers were always up to 100 000 euros and only within the EU, the bank will not evaluate this as a suspicious transaction which should be preventively blocked. What's more, the bank does not even have to report it to the authorities of the Slovak Republic.

And the last but not least, the problem with stopping these transactions is that the banks have usually one compliance or fraud officer who can stop these transactions and whose working hours are 8:00-16:00. Even the banks, with annual profits of several hundred million, allocate only one person who cannot be reached after working hours even by the police. This makes the 24/7/365 availability of FPS a great benefit for fraudsters. They can work at odd hours, especially when bank employees are not active. For this reason, victims may not be able to check their accounts and report fraudulent activity to the authorities in a timely manner.

> **Perceptions of cyber criminals must evolve; they're now professionalized and continuously refining their methods, resembling a service industry.**

HOW HAS AI CHANGED THE GAME?

In the standard scenario, the email account of a CEO was hacked and in his name the business partners are contacted that the bank account number has been changed, and all the payments are redirected the attacker's bank account. The new bank account is usually in a bank located in a third world country. It sounds too easy to fall for, but email communication is not the only thing AI helped to improve.

As attackers get more familiar with these technologies, we are going to see an increase in these attacks. The standard scenario using AI these days involves a deepfake videoconference call with CEO via nonstandard but still believable communication channels.

In one instance, attackers used WhatsApp to contact an employee, claiming the CEO urgently needed to speak with them. They then sent a MS Teams link for a videoconference. During the call, a deepfake CEO, appearing genuine, explained the CEO's absence and introduced a trusted associate to lead future communication. The goal was to extract confidential banking information. The only red flag was the use of MS Teams instead of the usual communication channel. Despite a minor typo in the contact name and a changed phone number, the employee failed to recognize the fraud.

WHAT MEASURES CAN YOU TAKE?

Awareness - Awareness and training significantly reduce probability of human error potentially causing high impact incidents. Perform regular phishing tests in your company.

Regulations and Internal Controls - Have a process in place where it is defined step by step which measures need to be taken when business partners are changing the bank accounts. Add several levels of controls, for example by making any transfer to a "new" bank account possible only if verified by a phone call. Include these measures into the Internal Control System and make sure that all involved parties are familiar with the process.

Banks and Insurance - Contact your bank in advance asking them what measures they have and who can be contacted 24/7. Verify if your insurance is covering such fraud.

BCM - Think about adding "CEO Fraud" to the scenarios in your Business Continuity Management and do regular BCM tests on this scenario, involving all your business partners. Emphasize that investing in preventive measures, even if initially costly, is usually worthwhile.

BE WISE, THINK TWICE, CLICK ONLY ONCE.

Perceptions of cyber criminals must evolve; they're now professionalized and continuously refining their methods, resembling a service industry. Employees and partners are vital to corporate security, necessitating regular cybersecurity education. AI and machine learning can also be harnessed and put to good use in the bank sector. AI can analyze transaction history and customer behavior to create user profiles, allowing for the detection and prevention of suspicious transactions through additional approval processes.