cfc

Case study

# CEO swindle

## A manufacturing firm transfers thousands to scam artists after falling victim to CEO fraud.

**Social engineering involves the use of deception to manipulate individuals into carrying out a particular act, such as transferring money, handing over confidential information, or clicking on a malicious link, and it's causing serious financial harm to businesses around the world.**

One of the most common types of social engineering is CEO fraud. This is typically a targeted attack where a fraudster impersonates the CEO or another senior executive within the organisation and instructs a member of the finance department to make an urgent payment to a particular account for a specific reason. More often than not, the CEO or senior executive in question will have had their email account compromised, but you don't even need to be hacked in order for this kind of fraud to be carried out. Some fraudsters will go off publicly available information, finding out what the CEO's email address is and amending it slightly before targeting a junior employee in the finance department who's often inexperienced and eager to impress his or her seniors. Many fraudsters will monitor social media sites and LinkedIn to see when the CEO or senior executive is away from the office to reduce the likelihood of having their scam uncovered.

Any business that transfers funds electronically can be susceptible to losses of this nature. One of our policyholders affected by a case of CEO fraud was a manufacturing company, specialising in the production of machinery used in the textile industry. As part of their business operations, the company utilized the services of a number of contract manufacturers that produce and supply specific component parts used in the firm's manufacturing processes.

## Credential phishing leads to inbox infiltration

The scam all began when the CEO fell for a credential phishing email. **Credential phishing emails are used by malicious actors to try and trick individuals into voluntarily handing over their login details**, typically by directing them to a link that takes them through to a fake login page. In this case, the CEO received an email from what he thought was Microsoft. The email stated that his account details needed to be validated in order for him to continue to use the Outlook service without disruption. As the email appeared to have come from an official source, the CEO clicked on the link. The link took him through to a seemingly legitimate landing page, where he inputted his email login details. Assuming that his account had been validated, **the CEO gave no further thought to the incident.** However, by inputting his credentials on this login page, he had actually passed on his details to a fraudster who could now access his account.

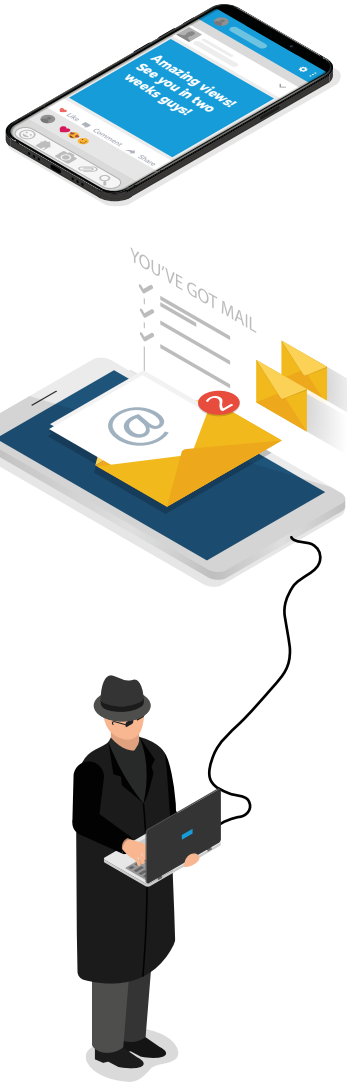
> Gaining access to the CEO's emails allowed the fraudster to gather information about how this company processed invoice payments

Gaining access to the CEO's email account allowed the fraudster to gather valuable information about how invoice payments were processed at this company. For example, **it allowed the fraudster to take a look at previous invoices** that had been sent from the insured's contract manufacturers and suppliers and to identify the main individual in the insured's finance department responsible for paying invoices and authorising wire transfer requests. What's more, it also allowed the fraudster to gain access to the CEO's Outlook calendar and establish what the CEO would be doing on any given work day.

Having worked out the CEO's schedule from his calendar, the fraudster waited until the CEO was travelling abroad for a few weeks on a business trip. With the CEO out of the office and with the chances of the scam being uncovered much reduced, the fraudster chose this moment to strike.

The fraudster's plan involved posing as a member of the accounts department for one of the insured's contract manufacturers.

**The fraudster's first step was to set up forwarding rules in the CEO's email account.** Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within a certain criteria are automatically forwarded to a specific folder or to another email account. In this case, **the fraudster set up two rules to ensure that the CEO didn't come across any of the emails related to the scam** whilst he was away on business. The first rule that was created meant that any emails from the individual responsible for approving payments were immediately marked as read and sent directly into the account's deleted items folder.




Forwarding rules ensure that certain emails are automatically forwarded to a specific folder or to another email account

The second rule meant that any email that included a keyword, such as "invoice" or words used in this particular contract manufacturer's trading name, in the subject line was marked as read and automatically sent to the deleted items folder.

# Phony invoices lead to unrecoverable funds

With the background work now done, the fraudster sent an email to the CEO purporting to be from the accounts department of the contract manufacturer, attaching an invoice for $47,500 and explaining that there had been a change of account details. To add an air of authenticity to the scam, the fraudster used one of the **actual contract manufacturer's invoices as a template.** So to all intents and purposes the invoice looked normal; it featured the contract manufacturer's logo and address on the heading of the invoice and carried a breakdown of the work carried out. The only difference was that the account details had been altered by the fraudster. As a result of the forwarding rules in place, this email was immediately marked as read and sent to the deleted items folder. The fraudster then logged into the CEO's account and, posing as the CEO, forwarded this email to the individual within the finance department responsible for authorising payments and requested that the payment be made that day. **As the CEO was out of the office and because the email requesting that the invoice be paid had come from his account, the employee in the finance department assumed that this was a legitimate request** and duly paid the invoice.

Having seen that this ruse had worked, the fraudster decided to try their luck and sent through another invoice a few days later. On this occasion, due to the fact that it had only been a few days since the last invoice had been paid, the employee in the finance department responded to the CEO about the request to check that this was correct. Because of the forwarding rules put in place, however, the CEO was oblivious to the employee's response – only the fraudster was aware of it. In the guise of the CEO, the fraudster responded and explained that all was in order and that the invoice should be paid.

With the employee in the finance department genuinely believing that they were in correspondence with the CEO and with any objections and queries about the payments being swiftly answered, **the fraudster managed to get two further invoices approved,** bringing the total amount paid out to $190,000. It was only upon the CEO's return to the office that the payments came up in discussion and the scam was uncovered. Our policyholder reported the incident to local law enforcement and attempted to recover the funds from the recipient bank, but all of the money had been moved out of the fraudulent account and the prospects of a successful recovery were deemed to be remote. Thankfully for the insured, however, they had purchased cybercrime cover on their cyber policy with CFC and were able to recover the loss in full.

## Our best defence against the rise in CEO fraud

This claim highlights a few key points. Firstly, **it illustrates how CEOs and senior executives are prime targets for cybercriminals.** CEOs and senior executives usually act as the face of their respective companies and as a result they tend to have bigger profiles on company websites and social media accounts, allowing cybercriminals to gather valuable information about them. In addition, cybercriminals know that employees are instinctively less likely to question and more likely to act upon instructions from senior executives. CEOs and senior executives therefore need to be especially conscious of sticking to good cybersecurity practices, and **employees need to be particularly alert to suspicious emails from senior executives** and have robust call-back and authentication procedures in place.

Secondly, it shows that cybercriminals are becoming much more sophisticated. In the past, it was not uncommon to see blatant attempts at funds transfer fraud over email, with an urgent appeal for help or bogus prize giveaways being just two examples. **Now, however, we are seeing far more nuanced attacks.** In this case, the fraudster managed to trick the CEO into volunteering his email login details, identify who was responsible for authorising payments and work out when the CEO was out of the office on a business trip, as well as setting up forwarding rules in the CEO's inbox to avoid detection and making use of one of the insured's genuine contract manufacturer's invoice templates to add authenticity to the scam.

Finally, this claim also discredits one of the most common objections that organisations have to purchasing cyber insurance: namely that by investing heavily in IT security, they have no need for cyber insurance. **The fact is that the vast majority of cyber incidents are a result of human error.** With increasingly sophisticated attacks like this on the rise, it makes it very difficult for employees to tell the difference between a real email and a fake email or a real invoice and a fake invoice. Furthermore, with more and more financial transactions being carried out electronically, the number of opportunities for cybercriminals to steal these funds has never been greater. Having good training and authentication procedures in place can certainly help reduce the risk of an event like this happening, but **it's impossible for any business to be completely impervious to these kinds of attacks.** This is why cyber insurance should be a part of any prudent organisation's risk management program, acting as a valuable safety net should the worst happen.