Case study

# Subcontractor scam

## Criminals swindle a construction firm out of large payment by impersonating a subcontractor

**Compared to many other industries, construction companies have been slower to take up cyber insurance. Because they typically don't hold large amounts of sensitive data and aren't solely reliant on their computer systems to carry out their business operations, construction companies don't often believe that they are overly exposed to cyber risk.**

Nevertheless, even if a business doesn't hold vast quantities of data or isn't wholly dependent on their systems to function, it is still likely that the business in question has some form of cyber exposure. Most modern businesses will hold some data on employees and third parties, use email to communicate with customers and suppliers, and use business bank accounts to receive and disburse funds electronically.

The construction sector is no different, and one area where they are particularly exposed is funds transfer fraud. Most construction companies will regularly work with suppliers and subcontractors to carry out their projects, and these partners will usually invoice the construction firm for the goods and services provided. If the company pays these invoices electronically, then they can fall prey to cybercriminals who are constantly looking for opportunities to intercept these payments and divert them to fraudulent accounts.

One of our policyholders affected by such a loss was a small construction firm with revenues below £50 million. The business specialises in commercial construction projects, ranging from office buildings to warehouse units and regularly makes use of specialist subcontractors to assist with projects.

# Digging for login credentials

The scam all began when an **employee 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 employee received an email purporting to be from Microsoft which stated that in order to implement some urgent new security features on his Office 365 account, he would have to verify his account details by clicking on a link. Not wanting to miss out on the new features, the employee clicked on the link and inputted his email login details. However, despite the email appearing to come from a legitimate source, **the employee had unwittingly handed his credentials to a fraudster.**

To make matters worse, **the construction firm had not enabled multi-factor authentication** on staff email accounts, so the fraudster was able to use the credentials to access this employee's email account remotely. This allowed the fraudster to monitor communications to and from the account and gain valuable information about the nature of the policyholder's business and the employee's role within it.

The employee whose email account had been compromised was one of the firm's project managers. As part of his role, **he regularly liaised with subcontractors and they would often send invoices over to him**, which he would then pass to the finance department for payment.

As it happened, a few weeks after the fraudster had gained access to the inbox, an email was sent over to the project manager from the managing director of a firm that had been sub-contracted by the construction company to carry out some structural steel fabrication work on a project. The email had an invoice attached for a month's worth of work done on the project, amounting to £93,425. Having spotted an opportunity, the fraudster chose this moment to strike.

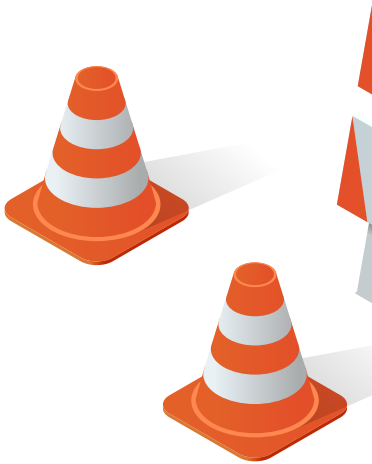
# Fraudster hammers out a plan

The first step was to set up a forwarding rule in the project manager's email account. Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within certain criteria are automatically forwarded to a specific folder or to another email account. In this case, **the fraudster set up a forwarding rule** that meant that any emails that featured the steel fabrication firm's genuine domain name were immediately marked as read and sent directly to the account's deleted items folder.

The next step was to **set up an email address impersonating the managing director** of the steel fabrication firm. In order to do so, the fraudster created an email address which, to the untrained eye, was exactly the same as the managing director's, but crucially omitted one character from the domain name. So rather than reading Joe.Bloggs@ABCfabricators.com, it read Joe.Bloggs@ABCfabicators.com.

The final step was to send an email to the project manager. In the email, **the fraudster explained that the firm had recently changed banks and that the previous invoice had mistakenly included the old account details.** The email went on to say that the new bank account details could be found on the new invoice attached to the email and that the construction firm should update its records so that all current and future payments went to the correct account.

**The fraudster had used exactly the same invoice template as before**, including the same company address, logo and statement of work, with the only amendment being the bank account details. In order to give the email an added sense of authenticity, the fraudster took the original email that had been sent by the subcontractor to the project manager and forwarded it on to the fake email account. The fraudster then replied to this original email when sending the fraudulent email to the project manager, making it appear as though it was part of the original email chain.



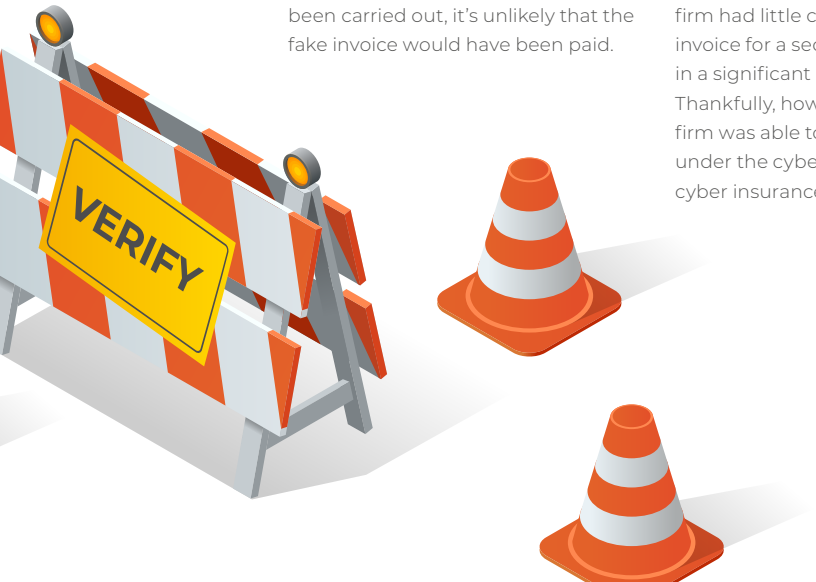
## Missed verification opportunity

With the email forming a part of the original email chain and coming from a seemingly identical email address, along with the exactly the same invoice template, the project manager never doubted the legitimacy of the request. Assuming that the change of account was valid, **the project manager sent the amended invoice over to the finance department for processing.**

In theory, it was at this point that the scam should have been thwarted. The construction firm had previously sent out an email to staff regarding the verification of account changes, stating that all requests for account changes should be followed up with a phone call to an individual at the company requesting the changes to confirm that everything was in order. If this verification procedure had been carried out, it's unlikely that the fake invoice would have been paid.

Unfortunately, **the member of the finance department dealing with the request failed to carry out this procedure** and updated the bank details, resulting in the full £93,425 being transferred to the fraudulent account.

It was only when the managing director of the steel fabrication firm called up the project manager, several weeks later, to enquire about the status of the payment that the scam was uncovered. Both the banks involved and local law enforcement agencies were informed about the loss, but by this point **it was too late and the funds had already been transferred out of the fraudulent account**. With the funds deemed unrecoverable and the steel fabrication firm still expecting payment, the construction firm had little choice but to pay the invoice for a second time, resulting in a significant loss to the business. Thankfully, however, the construction firm was able to recoup the funds under the cybercrime section of its cyber insurance policy with CFC.



## Smarter criminals and other key takeaways

This case highlights a few key points. Firstly, **it shows just how skillful cybercriminals are becoming at parting businesses from their money** and how difficult it is for businesses to spot a fake.

In this case, the fraudster managed to successfully impersonate Microsoft and manipulate the project manager into volunteering his email login details; set up a forwarding rule to prevent any emails from the real subcontractor reaching the project manager and jeopardizing the scam; set up a fraudulent email address that was virtually identical to the genuine subcontractor's; make it look as though the fake email sent to the project manager was part of the original email chain; and send over an identical invoice template to the one used by the genuine subcontractor.

Secondly, it illustrates how **human error plays a major role in cyber losses**. Many organizations don't think they need to purchase cyber insurance because they believe they have the IT security and risk management procedures in place to prevent a cyber loss. But as with so many cyber-related events, this loss stemmed from human error and it's very difficult for any business to eliminate this risk entirely. The fraudster was able to compromise the email account because the project manager fell for a sophisticated credential phishing scam, and the funds were successfully intercepted because an employee in the finance department failed to carry out a verification procedure.

Finally, it highlights how **almost all modern businesses have some form of cyber exposure**. Even though the policyholder in this case was a construction firm that didn't solely rely on its computer systems to carry out its business operations, the company still used emails to communicate with subcontractors and made payments electronically. All it took was for just one email account to be breached for the business to be defrauded out of £93,425. But by having a cyber insurance policy in place, **the company was able to successfully recover the loss**, illustrating the value that cyber insurance can bring to any modern business. ●