Case study

Recruitment ruse

When an employee at a recruitment firm falls for a phishing scam, a significant payment is misdirected

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

Any organisation that transfers funds electronically can be susceptible to social engineering attacks, which can result in the company mistakenly transferring funds to fraudulent third parties. However, it's not always businesses themselves that are tricked into transferring funds, but their customers. In some cases, fraudsters will impersonate a business, intercept communications between the business and a customer, and fraudulently redirect funds that were due to be paid to the business for the goods or services it provided. This can potentially result not only in strained relations with customers but also, in many cases, with the business being left out of pocket for the money that was owed.

One of our policyholders affected by such a loss was a recruitment and staffing firm. The firm provides recruitment services across a range of industries, including banking, insurance, manufacturing, and technology, and the positions that the company helps to fill range from entry level jobs to senior executive roles.

Credential phishing opens floodgates

The scam began when a member of the recruitment firm's accounts department 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 instance, the recruitment firm's employee received an email purporting to be from a spam filtering service. The email explained that some of the employee's outbound emails had been blocked by the spam filter, but it went on to explain that emails coming from the employee's account could be unblocked if the **employee clicked on a link and verified his email address by inputting his details.**

Not wanting to have a situation where important invoices to external clients were blocked by this spam filtering service, the employee clicked on the link and entered his email login details to verify the account. Unfortunately for the recruitment firm's employee, however, he had unwittingly handed his credentials to a fraudster.

To make matters worse, **the recruitment firm did not have multi-factor authentication enabled** for remote access to all company email accounts. This meant that the fraudster was able to gain access to the employee's account remotely without having to go through a second verification procedure, such as inputting a verification code or number. This allowed the fraudster to peruse the employee's email account, 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.

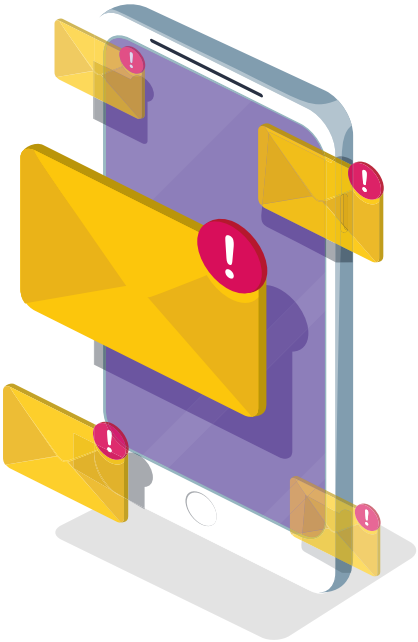
What the fraudster found was that as part of his role within the recruitment firm's accounts team, the employee was expected to send over invoices to client businesses following the successful placement of a candidate at the hiring company, with the recruitment firm charging a percentage of the newly employed candidate's salary as commission.

Spotting an opportunity, fraudster pounces

The fraudster was clearly looking for a lucrative opening to appear, and as it happened, the employee was in correspondence with a client business operating in the technology sector, whom the recruitment firm had recently helped in the hiring of a Chief Operating Officer. Following the successful placement of the candidate for the role at this company, **the recruitment firm's employee in the accounts department had sent over an invoice for £45,000 to the technology company.** Having spotted an opportunity, the fraudster chose this moment to strike.

The first step was to set up a forwarding rule in the employee'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 a forwarding rule that meant that any emails that featured the technology company's domain name were immediately marked as read and sent directly to the employee's deleted items folder.

The next step was to send an email from the employee's account to the technology company. In the email, **the fraudster explained that the recruitment firm had recently changed banks** and that the previous invoice had mistakenly included the details for the firm's old account. The email went on to say that the new bank account details could be found on the new invoice attached and that the payment for the recent placement of the Chief Operating Officer should be sent to the new account instead. ▶



In order to ensure that the request looked legitimate, **the fraudster used exactly the same invoice template as before,** including the same company address and logo, with the only difference being the addition of the new bank account details. The fraudster also ensured that the new email formed part of the original email chain, as well as adding some subtle touches, such as mimicking the employee's writing style and including the employee's email signature to sign off the email.

With the email forming part of the original email chain and coming from the recruitment firm's employee's genuine email address, along with the same invoice template as before, the individual responsible for processing the payment at the technology company never doubted the legitimacy of the request. Assuming that the new account details were valid, the client business paid the £45,000 owed and believed that the matter was now settled.

It was only several weeks later, when the recruitment firm's employee noticed that the invoice remained unpaid and contacted the technology company via phone, that the scam was revealed. The technology company contacted its bank and tried to see if the transfer could be recalled, but unfortunately it was too late and the funds had already been removed from the fraudulent account.

With the funds deemed unrecoverable, this meant that the money owed to the recruitment firm remained unpaid. However, as it was the recruitment firm's employee who had had his email account hacked, and as the request to change the bank account details had come from his genuine email account and appeared to be legitimate, **the technology company did not accept responsibility for the lost funds and was not willing to pay the invoice a second time,** leaving the recruitment firm out of pocket to the tune of £45,000.

Fortunately, however, the recruitment firm was able to recoup the lost funds under the cyber crime section of its cyber insurance policy with CFC, which provides cover for social engineering style losses such as this.

What these common crime claims teach us

This claim highlights a few key points. Firstly, it shows just how sophisticated cybercriminals have become. In the past, it was not uncommon to see blatant attempts at funds transfer fraud over email, with urgent appeals for help or bogus prize giveaways. **Now, we are seeing far more nuanced attacks.** In this case, the fraudster managed to gain access to the employee's email account by successfully impersonating a spam filtering service and getting the employee to input his login details on a fraudulent webpage, carefully selected a lucrative target, set up forwarding rules in the account to prevent the scam being uncovered, came up with a plausible reason for changing the account details to trick the recruitment firm's client, and added subtle touches to ensure the email appeared as legitimate as possible, such as using the same invoice template, mimicking the employee's writing style and including his genuine email signature.

Secondly, it highlights the importance of having multi-factor authentication in place on all business email accounts. Although the employee fell for the credential phishing email and handed over his login details, **it's highly unlikely that the scam would have gone any further had the recruitment firm had multi-factor authentication in place.** In addition, businesses should look to implement phishing training programs, which can help employees spot phishing emails.

Finally, this claim illustrates just how susceptible modern businesses are to funds transfer fraud losses. **With more and more businesses transferring money electronically, the opportunities for cybercriminals to intercept these transfers is increasing exponentially.** Indeed, businesses themselves don't even have to be tricked into sending money elsewhere to be affected. As this claim highlights, a business's customers can be duped into diverting legitimate payments intended for the business over to fraudulent accounts, potentially resulting in a loss to the business if the customer is unwilling to pay again. This is why cyber insurance, and cyber crime cover in particular, should be a part of any prudent organisation's risk management program, acting as a valuable safety net should the worst happen. ●