cfc

Case study

# Lucrative lookout

## A city government falls victim to a fraudster on the watch for sizeable wire transfers

**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 organizations around the world.**

Any organization that transfers funds electronically can be susceptible to social engineering attacks, and entities operating in the public sector are no exception to this. Public entities not only receive funds electronically in the form of grants from central government and tax receipts from local residents, but they also disburse large amounts of money both internally to different departments and externally to third party suppliers and contractors. All these transactions make for a tempting target for cybercriminals, who are constantly on the lookout for opportunities to intercept fund transfers and divert them to fraudulent accounts.

One of our policyholders affected by such a loss was a local government for a city with a population of around 140,000. The city government's responsibilities include public transportation, car parking facilities, social housing, parks and recreation areas, and recycling and waste disposal, and more.

## Fraudster glimpses prime opportunity

The scam all began when an employee from the city's finance 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 through to a fake login page.

In this case, the employee received an email purporting to be from Microsoft. The email explained that the employee's email account details needed to be verified in order for them to continue to use Outlook without disruption. With the email appearing to come from an official source and with the employee not wanting to suffer any disruption to her work, she clicked on the link included in the email. The link took her through to a **seemingly legitimate landing page with Microsoft branding in place**, where she inputted her email login details. Assuming that her account had been verified, the employee gave no further thought to the incident. However, by inputting her credentials on this login page, the employee had inadvertently passed on her details to a fraudster.

To make matters worse, the city government had not enabled multi-factor authentication on staff email accounts, so **the fraudster was able to use the credentials to access this employee's account remotely**. This allowed the fraudster to monitor communications to and from the account and gather valuable information about any upcoming transactions.

As it happened, the city government was in the process of building a new social housing development and had contracted a third party construction firm to carry out the building work on the project. **The construction firm would send regular invoices** for the work carried out to the city's finance department, who would then arrange for a payment to be made to the construction firm's bank account. The fraudster managed to find the email correspondence between the employee in the finance department and the finance director of the construction firm, and in the process the fraudster established that the latest invoice, totalling $213,456, had been sent over and was due to be paid within a few weeks. Having spotted a lucrative opportunity, the fraudster chose this moment to strike.

## Scam set up in a flash

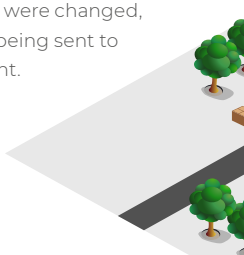
The fraudster's first step was to set up a forwarding rule in the employee's email account. **Forwarding rules are settings that can be applied to an email account** which ensure that certain emails are automatically forwarded to a specific folder or to another email account. In this case, the fraudster set up a forwarding rule that meant that any emails that featured the construction firm's genuine domain name were automatically 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 construction firm's finance director. **To the untrained eye, this was exactly the same as the finance director's**, but crucially omitted a character from the domain name. So rather than reading Joe.Bloggs@XYZconstruction.com, it read Joe.Bloggs@XYZconstuction.com.

The final step was to send an email to the employee in the city's finance department from this fake account. In the email, the fraudster explained that the construction firm's usual account was being audited and that meant that they were pausing all transactions while this was taking place. **The email then went on to explain that a temporary account had been set up** as an alternative and that all upcoming invoice payments should be sent there in the meantime, with the fraudster attaching a document with the new account details attached.

The fraudster also added some touches to the email to make it look as authentic as possible. For example, the fraudster forwarded the original email correspondence between the city government's employee and the construction firm's finance director to the fraudulent email address, with the fraudster then responding to this email correspondence and making it look as though the fake email was part of the original email chain. The fraudster also **signed off with the finance director's genuine email signature** and the document with the fake account details featured the construction firm's genuine logo and address details.

With the fraudster's email forming a part of the original email chain and coming from a seemingly identical email address, along with a plausible excuse for changing the account details temporarily, the employee in the city's finance department **never doubted the legitimacy of the request** and the construction firm's account details were changed, resulting in $213,456 being sent to the fraudulent account.



## Discovered too late

It was only when the construction firm's finance director called up the city's finance department a few weeks later to enquire about the status of the payment that the scam was finally uncovered. The banks involved and local law enforcement agencies were immediately notified about the scam and attempted to recover the loss, but by this point it was too late to retrieve the funds as they had already been transferred out of the fraudulent account.

With the lost funds deemed unrecoverable and the construction firm still expecting its invoice to be paid, **the city government had no choice but to pay the invoice again**, resulting in a significant financial loss.

Thankfully, however, the city was able to recoup the stolen funds under the cybercrime section of its cyber policy with CFC, which provides cover for social engineering-style losses such as these.

## Follow-up with a call and other key takeaways

This case highlights a few key points. Firstly, it illustrates why **any organization that is undertaking a construction project should be extra vigilant** when it comes to funds transfer fraud. Cybercriminals know that any construction project is likely to require sizeable transfers of money, which makes it a particularly lucrative and tempting area for them to target. Any organization involved with a construction project, whether it's the entity that's paying for the project or the contractors carrying it out, should be on their guard to prevent funds being intercepted by fraudsters.

Secondly, it shows just how skillful cybercriminals are becoming at parting innocent organizations from their money and **how difficult it is to spot a fake**. In this case, the fraudster managed to successfully impersonate Microsoft and manipulate the city's employee into handing over her login details; set up a forwarding rule to prevent any genuine emails from the construction firm from reaching the employee and jeopardizing the scam; set up a fraudulent email address that was virtually identical to the construction firm's finance director's address; make it look as though the fake email sent to the employee was part of the original email chain; and make use of the finance director's genuine email signature and the construction firm's logo and address on the document containing the fake account details.

Finally, it highlights the importance of having call back procedures in place. Call back procedures work by ensuring that whenever a new payee account is set up or a change of account is requested, **the request is verified by having a member of the accounts department call the person or company requesting the change on a pre-verified number to confirm that it is legitimate**. If the city's finance department had had this procedure in place and the employee had followed it, it's highly unlikely that the funds would have been intercepted. Having call back procedures in place, alongside staff training on phishing risks and multi-factor authentication on email accounts, can significantly reduce an organization's exposure to funds transfer fraud. Nevertheless, it's worth noting that none of these methods are fool-proof and it's very difficult to eliminate this risk entirely, especially when human error is factored in. And that's why cyber insurance can be such a useful purchase, providing a valuable safety net when things go wrong. ●