Case study

Donation diversion

A charity's payment to a research partner is sent to a fraudulent account after an email is compromised

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.

Any business that transfers funds electronically can be susceptible to social engineering attacks, and those organizations that operate in the charity sector are no different. Most charities will not only receive funds electronically in the form of donations, but they will also often be involved in the disbursal of funds to third parties to help carry out their charitable projects.

One of our policyholders affected by such a loss was a cancer charity. As part of the charity's business operations, they regularly transfer money to businesses and universities that are involved in medical research aimed at tackling cancer.

Controller tricked into handing over credentials

The incident all began with a business email compromise (BEC) at a third-party medical research company. **The charity had been funding a number of research projects** that were being undertaken by this company, and had been sending over money on a monthly basis.

In this instance, the medical research company's financial controller received an email purporting to be from Microsoft's Office 365 support service. The email stated that Office 365 had prevented the delivery of some new messages, but went on to explain that the financial controller could release these emails by clicking on a link and entering his login credentials. Wanting to ensure that he wasn't missing out on any important emails, the financial controller clicked on the link. The link took him through to a seemingly legitimate landing page, **at which point the financial controller inputted his login credentials.**

Unfortunately, this was not a genuine message from Microsoft, but a credential phishing email.

By entering his login credentials on the landing page, **the financial controller had inadvertently passed on his details to a fraudster.**

> "Wanting to ensure that he didn't miss out on important emails, the financial controller inputted his login credentials on the seemingly legitimate Microsoft Office landing page."

To make matters worse, the medical research company had not enabled multi-factor authentication on employee email accounts, allowing the fraudster to access the financial controller's account remotely. This meant the fraudster could peruse his inbox and monitor any communications to and from it.

Account takeover results in diverted payments

While browsing the inbox, the fraudster came across some regular email correspondence between the financial controller and a member of the charity's accounts department, in which the financial controller would typically send over a monthly invoice for work carried out on the research project. Realizing that it might be possible to intercept some of these regular payments, **the fraudster looked to exploit this opportunity.**

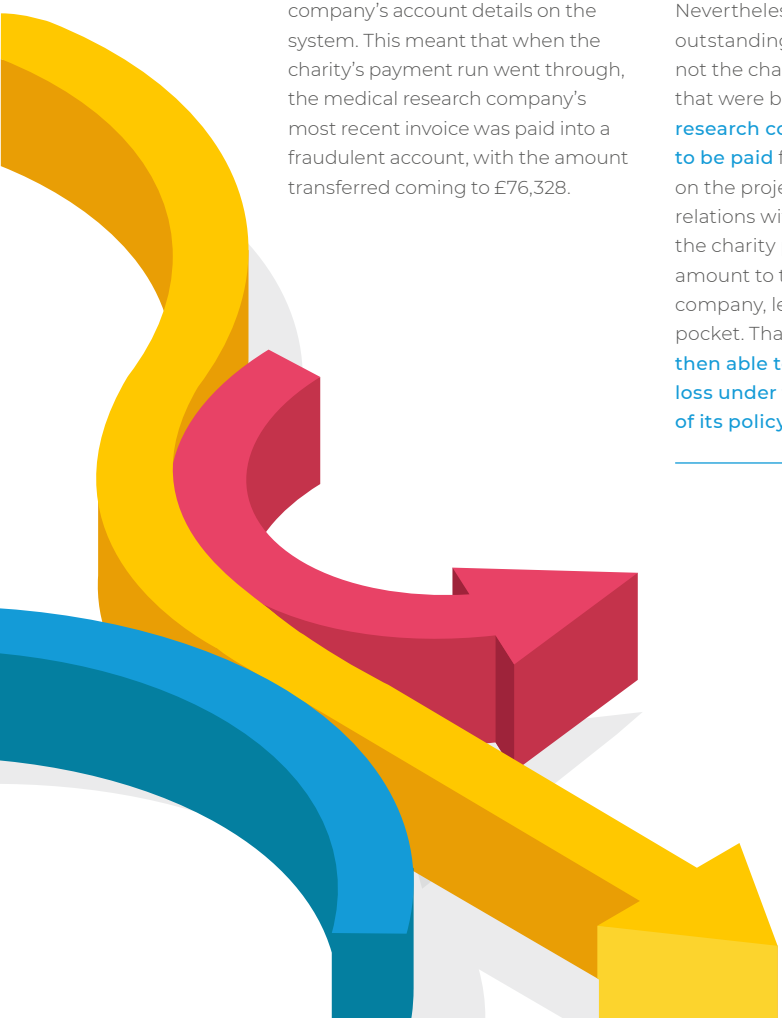
The fraudster began by setting up a forwarding rule in the financial controller's email account. Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within a set criteria are automatically forwarded to a specific folder or to another email account. In this case, **the fraudster set up a forwarding rule** that meant that any emails that featured the charity's domain name were immediately marked as read and sent directly to a pre-existing folder within the financial controller's email account that had been dormant for several years.

The next step that the fraudster took was to send an email over to a member of the charity's accounts department from the financial controller's genuine email account. In this email, the fraudster stated that the medical research company had **recently taken the decision to move to a different banking services provider.** The email included an attachment containing the new banking details and went on to explain that all pending and future invoice payments should be sent to the new account with immediate effect. To give these instructions a veneer of legitimacy, the document containing the new account details included the medical research company's logo and address, as well as the name, title and contact details of the financial controller.

With the email coming from the financial controller's genuine email address, and with the document containing the new bank account details having an air of authenticity, the employee working in the charity's accounts department assumed that this was a legitimate request and amended the medical research company's account details on the system. This meant that when the charity's payment run went through, the medical research company's most recent invoice was paid into a fraudulent account, with the amount transferred coming to £76,328.

It was only when the financial controller called up the charity to chase up the invoice payment a week later that the scam was uncovered. Both the banks and local law enforcement were informed about the loss, and fortunately one of the banks was able to claw back £27,653.

Nevertheless, this still left £48,675 outstanding, and even though it was not the charity's computer systems that were breached, **the medical research company still expected to be paid** for the work carried out on the project. Not wishing to strain relations with one of its key partners, the charity paid the remaining amount to the medical research company, leaving the charity out of pocket. Thankfully, **the charity was then able to recoup the £48,675 loss under the cybercrime section of its policy** with CFC.



The human element of cyber risk and more

This claim highlights a few key points. Firstly, it shows 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.** In this case, the fraudster was able to compromise the medical research company's computer systems because its financial controller fell for a sophisticated credential phishing scam, and the funds were successfully intercepted because an employee failed to verify the account change using a method other than email.

This highlights another important point when it comes to cybercrime: the value 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 charity had had this procedure in place and the employee working in the finance department had followed it, it's highly unlikely that the funds would have been intercepted. Although there is no fool proof method of preventing funds transfer fraud, implementing call back procedures can certainly reduce the risk for businesses.

Finally, it represents a shift in the nature of cyber risk for the charity sector. As charities will often collect personal data, such as names, addresses and payment card information, in the course of their business activities, they have often seen their cyber risk primarily in terms of the risk of a data breach. However, with the rise of social engineering style attacks, **organizations that operate in the charity sector can no longer afford to focus exclusively on data breaches** when managing their cyber risk. With many charities both receiving and disbursing electronic funds on a regular basis, charities should ensure that they are alert to the risks and have effective cybercrime coverage in place. ●