Case study

School fees fiasco

Parents mistakenly pay tuition fees to a fraudster impersonating a private school

Educational establishments have typically seen their cyber exposure in terms of the risk of suffering a data breach. This is due to the fact that they will often hold sensitive data on both students and their parents and are aware of the potential regulatory obligations that a breach of that data might impose upon them. However, educational establishments shouldn't see their cyber exposure as being exclusively about data and privacy risk.

Funds transfer fraud – whereby fraudsters dupe innocent businesses and individuals into transferring what they believe are legitimate payments to fraudulent bank accounts – is becoming an increasingly common problem for most modern organizations, and this includes those operating in the education sector.

In an insurance context, most cyber policies with crime cover in place will provide some form of protection for situations where policyholders lose their own money in this way. For example, if a fraudster manages to impersonate a school principal and gets a member of the finance team to send a payment over to a fraudulent bank account, the policyholder's business will have suffered a financial loss. Usually, this loss can then be recovered under their cyber policy.

However, it's not always the policyholder's business that suffers a loss in this way, but the policyholder's customers. Customer payment fraud describes a situation in which a business is impersonated by a fraudster, who then dupes some of the business's customers into making payments to a fraudulent account.

One of our policyholders affected by such a loss was a private, tuition fee-paying school responsible for educating 11-18 year olds. The school in question has boarding facilities in place and attracts students from many different countries around the world.

Lack of multi-factor authentication lets fraudster in

The scam began when the school's bursar, the individual responsible for managing the financial affairs of the school, 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 bursar received an email from what appeared to be Microsoft, stating that if he wanted to continue to use the email account without interruption, he would have to validate his account details online. Not wanting to face any disruption to his work, the bursar clicked on the link provided, which took him through to an authentic-looking landing page where he inputted his email login details and gave no further thought to the matter.

Despite appearances, however, the landing page was actually fake, and the bursar had unwittingly volunteered his email login details to a fraudster. **What's more, his email account didn't have multi-factor authentication in place**, so the fraudster was then able to access the account remotely and gather valuable information. In particular, the fraudster was able to locate a spreadsheet stored in one of the bursar's email folders containing a list of email addresses for the parents of current students, which was typically used for distributing general messages and updates from the school.

Did you know?

MFA is an authentication process that is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Most cases of business email compromise could be prevented by implementing it.

Scam initiated with offer of discount

Having spotted an opportunity, the fraudster moved on to the next stage of their scam. Their first step was to set up an email address that looked substantially similar to the bursar's, but with the addition of an extra letter to the address line. So instead of saying @abcschool.com, it became @abcscchool.com. **The next step was to carefully select which parents to target**. Rather than adopting a scatter gun approach and emailing every parent on the list, the fraudster specifically selected parents based overseas. This was presumably done not only on the basis that such parents are more likely to be paying both tuition and boarding fees (thereby making them more lucrative targets), but also in the belief that overseas parents might be more likely to fall for the scam and less likely to raise the alarm to the school.

With the targets selected, the fraudster sent out an email relating to the payment of school fees. The email began by outlining what the annual fees for tuition and boarding amounted to, but then stated that parents would be eligible for a discount of up to 25% if they paid for the spring and summer terms in one lump sum as opposed to paying separately at the start of each term. To add a sense of urgency to making a payment, the email then went on to say that **there was a deadline for payment in place**, after which the discount would expire. Social engineering attacks rely on manipulating and exploiting typical human behaviours, and in this case the fraudster was clearly aware that the scam would have a better chance of success if the parents were provided with a financial incentive to make the payment within a set time frame.

In addition, the email was well thought through and **included a number of features to make it appear more authentic**. For example, not only did the fraudster use proper spelling and grammar and include the bursar's genuine email signature, he also went on to state that if the student was unable to complete the academic year for whatever reason, then the fees would be reimbursed on a pro-rata basis.

School's security breach puts parents out of pocket

Unfortunately, this offer proved to be too tempting for some and six parents fell for the scam, transferring the tuition and boarding fees over to the fraudulent account details provided on the email. With tuition and boarding fees at the school costing some $10,050 per term, **the amount paid out by each parent at a 25% discount amounted to some $15,075**.

It was only after a few days, when one of the parents that had received the email forwarded it to one of the school's administrators to check the validity of the discount offer that the school became aware of the scam. The school immediately notified all parents about the scam and urged them to be aware of any suspicious emails that appeared to have come from the school.

> Of the six parents affected, just two were able to get their money back, with the rest left out of pocket to the tune of $60,300 collectively.

The parents that fell for the scam reported the incident to their respective banks to see if the transaction could be either frozen or reversed, with mixed results. Of the six parents affected, just two were able to get their money back, with the rest left out of pocket to the tune of $60,300 collectively.

As it was a compromise of one of the school's email accounts that had allowed the fraudster to gain access to the parents' email addresses, **the school felt morally obliged to reimburse those parents** affected by the fraud. Fortunately, the school was then able to recoup most of this loss under the cyber crime section of its policy with CFC, which provides cover for customer payment fraud up to a maximum of $50,000.

Lessons learned

This claim highlights a few key points. Firstly, it shows just how skilful cybercriminals are becoming at parting individuals and businesses from their money. In this case, the fraudster managed to successfully impersonate Microsoft and **lured the school's bursar into volunteering his login details**; took his time to peruse the inbox and locate a spreadsheet containing parents' email addresses; decided to specifically target overseas parents rather than adopting a scatter-gun approach which might have raised the alarm and seen the scam uncovered sooner; offered a discount within a limited time range to induce parents to transfer the tuition and boarding fees promptly; and included a number of small touches, such as the use of the bursar's genuine email signature, to make the email look and sound as authentic as possible.

Secondly, it represents a shift in the nature of cyber risk in the education sector. Educational establishments have long seen their cyber risk as being primarily about privacy. However, with the rise of social engineering style attacks, organizations that operate in the education sector can no longer afford to focus exclusively on data breaches when managing their cyber risk. **Private schools in particular should ensure that staff are aware of phishing scams** and make sure that parents are alert to any suspicious communications that might appear to come from the school.

Finally, it highlights the need for customer payment fraud cover in cyber policies. Many cyber policies with crime sections will only provide cover for losses that directly affect a policyholder. But in this instance, **it wasn't the school that suffered a direct loss but its customers**. However, because it was a compromise of the school's computer systems that allowed the attack to be carried out, the school felt duty bound to reimburse the parents affected. With more and more financial transactions being carried out electronically and with more and more cybercriminals looking to intercept them, the chances of a business's customers falling for scams of this nature are only increasing and it's usually the business that has been impersonated that will take the blame. That's why it's a good idea to check your cyber policy for customer payment fraud cover.