The weakest link

Summary
- Trustees are at risk of being scammed, particularly through phishing emails, due to the large amounts of data they can access.
- Education and training as to the nature of phishing scams can help prevent trustees from succumbing to them.
- Regular monitoring is also recommended.

The success of cyber attacks is largely down to human error, so are trustees aware of the personal risk they may be to the pension scheme they manage? And what steps can be taken to reduce the likelihood of trustees falling for a phishing scam? Laura Blows finds out

Ninety per cent of cyber breaches in 2019 were caused by human error, recent research by CybSafe finds. For all the sophistication of cyber attacks, and their connotation with technological advancement, and for all the clever programmes and significant money spent to counteract them, the vast majority of their success is simply down to the weakest link in the chain: us.

Awareness of the human propensity for scams is nothing new. The pensions industry has dedicated much effort on trying to protect its savers from falling victim, providing communications and services to educate them on the signs they may be being targeted by criminals. But has enough thought been given to the idea that the trustees of pension schemes themselves may be at risk of fraud?

Trustees targeted

According to The Pensions Regulator's (TPR) April 2018 *Cyber Security Principles for Pension Schemes*, pension schemes hold large amounts of personal data and assets that can make them a target for fraudsters and criminals.

As they deal with financial matters, trustees may consider themselves less likely to believe a fraudulent claim, particularly one requesting money. Yet "research shows that finance professionals and others who are more financially literate may be more prone to falling for scams", PLSA policy lead for lifetime savings, George Currie states.

"While trustees are increasingly alive to member transfer scams, it is important that they recognise the threats posed to schemes and their trustee boards directly," Dalriada Trustees professional trustee, Tom Lukic, says. "Scams can take a variety of forms, from opportunistic fraudulent benefits payments perhaps made after a member or dependent dies, through to large scale 'professional' cyber data thefts."

Most individuals are aware of cyber data thefts in the form of scam emails, Aon partner, Paul McGlone, says. However, he adds, some trustees are not aware how this could impact on their role and the scheme. "Trustees working for large corporations will get regular training on phishing emails and other types of scams, but trustees working for smaller companies or as an individual may not have the same levels of awareness."

Gone phishin'

A phishing email is an attempt to trick the recipient into giving, or following a link that will give, data to a cyber criminal. In 2019, 45 per cent of security breaches reported to the Information Commissioner's Office related to phishing emails.

According to Pasa's cyber expert company Crowe UK's national head of forensic services, Jim Gee, phishing emails usually try to elicit confidential or personal information illegitimately, induce improper payments, infect or encrypt the recipient computers.

To do this, a trustee may receive a phishing email containing fake invoices or requests from service payments. They may also get false requests for information from scammers posing as scheme members that could be used to commit identity theft – according to Taylor Wessing senior associate, Jo Joyce, this targeted form of email scam is often called 'spear phishing'.

"While some phishing emails directly request something (eg payment), many don't," McGlone warns. "The main aim is to hijack trust, which might lead to the recipient clicking on a link or opening an attachment. That can infect their computer and in turn provide a route into their email contacts and their systems."

Look out

So how can a trustee tell between a legitimate email and a false one?

There are a number of things trustees can look out for, such as a message that encourages prompt action (to reduce time for the email to be properly considered) or asks for personal data or passwords, misspellings in the email text, the 'reply to' email address being from a different domain to the sending one, or the email signature/formatting being different from the norm, if it is pretending to be from a regular contact. In this instance, another popular tactic, Davis states, is to use 'travelling overseas' as an excuse not to send the request through normal channels. An email from someone involved in the scheme coming out of the blue is another cause for concern.

Knowing these warning signs may help, but Joyce warns that phishing scams are becoming increasingly sophisticated and hard to spot. "The days of poor English and obviously faked email addresses are giving way to very plausible scams."

Impact

If a trustee does fall for a phishing scam, the threat to the scheme is that they are a point of access, McGlone says. "For example, if they can be impersonated through a compromised email account then that may provide a route into their third-party administrator or investment managers. At that point the scheme's data and assets are at risk."

Enabling a serious breach through neglect or negligence may amount to a breach of fiduciary duty, Joyce warns, "but the reputational damage that arises from falling prey to a scam may be far more serious than the legal consequences".

One such scheme that has suffered the consequences of falling prey to fraud is Nest. In its annual reports and accounts for 2013/14, it was revealed that it had been subject to a mandate fraud loss of £1.4 million from its operating budget, involving the diversion of payment to a supplier, with no money taken from members pots. The auto-enrolment provider subsequently managed to retrieve £0.3 million of the missing funds.

Commenting on this, its CEO at the time, Tim Jones, said: "We have taken measures to reduce the risk of fraud by strengthening our processes, doing a root and branch review of all our procedures and by updating our training for staff on fraud risks."

Prevention

To help ensure such a scam does not occur again, Nest chief risk officer, Dan Davis, says: "We have a robust approach to ensure our trustees are protected from phishing scams. This includes an intelligence-based solution, with a regular programme of staff awareness training and a software-based solution that monitors for cyber threats, such as dodgy links, and responds proactively."

Trustees are particularly vulnerable to phishing scams when they are using personal email addresses that do not benefit from the more sophisticated security measures used by large corporates, Sackers senior associate, Oliver Topping, notes.

For this reason, McGlone advises trustees set up a separate email account specifically for scheme work, to limit the number of people who know it and to make it easier to identify emails that should not be there. Scheme contacts from non-scheme email accounts should also be cleared, he adds.

TPR's principles recommend ensuring there are controls around the trustees' work, such as having clear policies on what can and can't be sent to personal email addresses or accessed on tablets or mobile phones, while Joyce adds that the use of multi-factor authentication when using mobile devices is rapidly becoming a must.

Despite these efforts, suspicious emails may occur. In these instances, Gee warns, check the sender's email address and do not click on links in an email. Instead, type them into the search bar or Google and check that the URL contains 'https://' and a green padlock. Also, it may be worth calling the contact to confirm if they did really send the message.

Training

While these tips and tricks are useful, specific training on the matter may help trustees fully comprehend the risks they face and how to mitigate them.

Yet, according to Topping, "while some trustees have received training from their advisers on cyber security as part of their work to comply with the General Data Protection Regulation, this isn't the case across the board in our experience".

According to Gee, Crowe has provided cyber crime awareness training for trustees from several pension schemes. "This usually blends training about their personal cyber security and resilience, but also can include cyber crime scenario-based training."

In early 2019, Aon approached its clients to see if they would be interested in participating in a group phishing campaign. Thirty-five pension schemes of varying sizes, featuring 250 trustees of all types – member-nominated, corporate, professional – agreed for Aon to send them a fake pensions-related phishing email in the second half of the year. In some instances all trustees were aware of this, for others only the trustee chair knew.

According to McGlone, different trustees faced different challenges.

As corporate trustees have firewalls installed, the fake email was less likely to reach a corporate trustee than a member-nominated trustee (MNT), McGlone states, but a "MNT was less likely to open an email to do with pensions that comes to their home address as they don't tend to get them that often, making

War games

For training purposes, trustees, professional trustee firms or in-house pension departments can undergo simulation exercises of a cyber attack.

For a few years, Aon has been offering these 'war games' to schemes of all sizes, primarily to raise awareness of the consequences that may occur, but also to test a scheme's incident response plan.

Over the course of an hour, the participants receive regular information about a cyber-attack scenario and how it is developing. A data breach is the most common, but other circumstances, such as a critical systems failure or an asset loss may also be reenacted. The situation during the hour may get worse, with situations such as member complaints, the media getting wind and an insurance claim occurring.

The developments are usually conveyed in written form, but more sophisticated methods, where voicemails from an administrator, a letter from an MP or a mock up of a news article, for example, can also be used.

The simulation is most effective face-to-face, although dial-ins are possible. It may also interact with the scheme administrators, advisers, actuaries and lawyers. Discovering how much support the sponsor will provide in such a scenario is also interesting, as "it may be the trustees' data and assets, but it's actually the sponsor's reputation on the line", McGlone says.

"You realise some things are more of a priority than others," he adds. "If you mention the possibility that pension payroll needs to be cancelled, that gets everybody's attention, as the idea that pensioners won't get paid is horrendous."

Another common occurrence is that everybody agrees that the members need to be communicated to, but it is difficult to agree what to tell them. "Do you tell them there's been a possible breach, when do you tell them, do you say whether they specifically have been affected, or not mention it and just say generally about not taking risks with their data?" McGlone says.

He recalls splitting a team into two groups, one handling a data breach and the other an asset loss. "At the end, they all agreed, while no one likes having missing money, at least the impact is contained, it's a set loss, while losing data could spiral out into many different directions."

The feedback of these simulations is always positive, McGlone says, with participants enjoying the interactive element and the scheme-specific scenario testing.

them more suspicious". Meanwhile, a professional trustee receives pensions emails all day, every day, making it much harder for them to identify the fake one.

Despite these challenges, the overall take-up rate came back lower than the general average of 20-30 per cent for these tests. Some schemes got an impressive zero take up, while others were higher than average.

For those, McGlone says: "There are a few raised eyebrows across the room, with everybody looking at everybody else, thinking as a group we have failed, but it is better to have failed in this environment where it was a fake, than fail on a real one."

Aon will be running another such exercise this year. It approached the schemes that took part in the inaugural one to see if they wanted to take part again, and according to McGlone, over 50 per cent came back within a couple of days to say yes.

Continual monitoring

Nest is an advocate of this style of prevention, Davis says, with appropriate training to spot phishing emails being conducted annually with all its staff, including trustees.

"Two or three years ago, the idea that a phishing scam would be on the agenda of a trustee meeting just wouldn't happen," McGlone states, "whereas now it is one of a number of things trustees talk about when thinking of security."

As Joyce says: "Trustees must remember that the greatest risks arise from human error and so regular training on spotting scams is crucial. The use of internal phishing emails to test that training will also provide a reminder of the need for ongoing vigilance and also to test the effectiveness of the training."

Through this education, training and ongoing vigilance, people may no longer be such a weak link in the chain protecting against scams.

Written by Laura Blows