THE RISE & RISE OF SOCIAL ENGINEERING FRAUD – DO YOU BELIEVE IN FAKE NEWS?

Social engineering fraud has been around for some years now and it is widely recognised that the consequences of falling victim to a scam can be devastating. Last year we issued a bulletin highlighting this growing problem and giving guidance on how to avoid becoming the fraudsters' next victim. [Bulletin 2019/01] So the problem itself is not a new one. What has changed is that the number of these attacks has risen at an alarming rate during the COVID-19 pandemic. Cybercriminals have spotted an opportunity and are taking full advantage of the sudden shift to remote working, and the increase in payments being made electronically.

This bulletin shares some of the recent experiences of Griffin Members, to help raise awareness across the membership of the increase in this particular risk. We also take this opportunity to give a reminder of some of the practical steps Members can take to try to avoid falling victim to a scam.

What is social engineering fraud?

Social engineering fraud is where a criminal manipulates an individual into revealing confidential information. The information sought varies but people are commonly tricked into revealing passwords or bank account details, or into giving access to their computer, where the criminal will then install malicious software. In the current climate, criminals seem to consider it an easier win to exploit people's natural inclination to trust what they are told, rather than go to the trouble of hacking their software.

This kind of criminal activity affects all businesses large, small, public or private. The German Health Authority, for example, nearly paid out Eur 2.4m this year for face masks which were never received. Experienced buyers found themselves embroiled in a web of referrals, fake e-mails and fake websites. Transfers of funds were intercepted and, whilst there are understood to have been some recoveries, the trail was complex and involved five different countries.

For intermediaries, the obvious risk is that they will pay claims or premium monies over to criminals after receipt of fraudulent banking information. Likewise they may unwittingly transmit erroneous bank details to a client, to enable the client to pay an insurer or other party directly, but the client will then in fact pay a fraudster. A different risk may present itself where it is the client that is duped and it then seeks some redress under cover which has been placed by the intermediary. The intermediary will need to have been clear about the scope of cover under the policy, and any exclusions for issues such as social engineering fraud, at the time of placement, to avoid becoming a target itself of an already distressed client.

War stories from Members and their clients

The tactics used by cybercriminals are increasingly sophisticated but many have one simple aim – to divert a payment, which it is known is about to be made, from the intended bank account to an account belonging to the fraudster. In each of the following instances, the Member has been tricked into accepting fraudulent instructions to change the bank account to which a payment is made:

War story 1

A sum equivalent to £1million was recently diverted in this way. The Member had placed a binding authority agreement on behalf of a coverholder. The coverholder had issued a professional indemnity policy to a consulting firm under the binder. The consulting firm was engaged in a dispute and settlement was agreed. The Member collected funds from underwriters to pay the settlement. They were provided with a settlement agreement containing bank details. Shortly after, the Member received an e-mail purporting to be from the coverholder with different bank details. The e-mail was in fact from a fraudster with small changes to the domain suffix – the addition of a dash and addition of ".com" at the end. The fraudster had also provided a doctored version of the settlement agreement. Subsequent to payment being made, e-mails with proof of payment were intercepted and e-mails were sent out impersonating the Member. Fortunately in this instance the quick action of the Member, the managers and overseas lawyers instructed at short notice to assist, once the fraud was discovered, resulted in the funds being frozen in the fraudster's account before they could be dissipated.

War story 2

In another matter, a Member, who had been provided with certain overseas bank details asked their client, a producer, specifically for US Dollar account details to facilitate a payment. The Member was, in fact, advised of new bank details from a fake sender, purporting to be the producer. The Member transmitted the monies to this new bank account. The producer received fake e-mails which it thought was from the Member and so had been led to believe monies would be in its account. On that basis the producer remitted payment to its client, a reinsured. The fraudsters, when sending the fake "Member" e-mails, had simply swapped two letters around. The monies had not, in fact, reached the producer's account as they had been transmitted to the fraudulent account. The Member had a criminal insurance policy in place but this required it to verify new bank account details by way of a telephone call. The Member had not done so and, as a result, whilst that policy paid out in part, there was a discount applied.

War story 3

A further example involved a Member receiving a premium invoice and, shortly after, receiving another with different details asking that monies be paid into a Portuguese bank. The Member passed on the "fake" invoice to the client without any checks taking place. Whilst some areas of the Member's business had procedures involving telephone checks on the veracity of invoices, this particular business area had no such checks since it was not itself going to be paying any monies out. The client paid over premium monies directly to what it believed was the insurer bank account. The observable change in the e-mail address used to send the invoices was subtle - simply an alteration whereby the suffix ".org" was used as opposed to ".com". In the course of the fraud, e-mails were also sent from a fake Member domain and the Member had to contact the domain registry to get this taken down.

In some instances it has been the Member's client, rather than the Member itself, that has been duped.

War story 4

One Member encountered a situation where an overseas insured was the victim of a social engineering fraud. A few letters were changed in the address of an e-mail sending "new" bank details and the insured paid an invoice using the fraudulent details. A problem subsequently arose for the Member when the insured tried to recover its loss by claiming on a policy placed on its behalf by the Member, as insurers refused to pay the claim. The Member faces allegations that the cover which they were involved in procuring was inadequate.

War story 5

We are also aware of a situation where the e-mail account of a Member's client was impersonated by fraudsters. The client had negotiated a deal to sell a valuable item but the email addresses of both the Member's client and the purchaser had been compromised by fraudsters. At one point during the sale negotiations, a member of staff at the purchaser's business had used a personal rather than business email address, which undoubtedly will have created a weak link. The result was that the purchaser transferred substantial funds (over £2m) to the fraudsters instead of to the Member's client.

What are the clues to look out for?

These attacks are increasingly sophisticated and so it is understandable that people are being caught out. The changes to e-mail addresses used are often very subtle; in one instance, three upper case letters in the name were changed to lower case and there was an addition of an extra "dash". In another situation, various people were "cc'd" into e-mails. These were purportedly from the Member's genuine client but there were changes to the suffix of the full e-mail address. This would be difficult to spot and meant that, as communications regarding payments progressed, the fraudsters were able to effectively "jump in" at the opportune moment. Other devices used have included registration of spoof domains and false registration of senders associated with legitimate domains.

Whilst many of the tricks used are difficult to spot, there are still a number of tell-tale signs that can serve as an alert to a potential victim. One potential clue to a fraudulent e-mail is where a correspondent who is normally fluent in English (or another language frequently used) becomes more stilted, or where there is simply a change in their usual tone or manner. Poor grammar or unusual spelling errors can also be a give-away.

Suspicions should also be raised if two or more e-mails are received from the same person with similar content but different despatch or receipt times. In one of the examples referred to above, a genuine e-mail was sent relating to the transmission of funds. This was followed, less than ten minutes later, by an e-mail from the fraudster indicating that the earlier e-mail was not meant for the client and effectively had been sent in error. This device effectively bought time for the fraudsters – it stopped the client checking its account and thus the fraudsters had more time to get the monies out of the fraudulent account.

Another red flag is where something suddenly needs to be done without previous warning and with a great sense of urgency. Fraudsters often try to instil a sense of urgency and pressurise entities to get things through quickly, which may lead to shortcuts in the usual due diligence.

One device commonly used in scams is what is referred to as “fake president fraud”. This involves a fraudster taking on the identity of one of the senior management team. An employee, often in the accounts team and responsible for making payments, is then contacted usually by phone or email. The employee is instructed to make an urgent and confidential payment to a third party and is given bank account details so that the payment can be processed. This is then accompanied by a credible cover story as to why the payment needs to be made and why it is essential it remains confidential. Once the payment is made the funds are swiftly moved on by the fraudster. All accounts staff should be reminded that they will never be criticised for following the firm’s procedures, regardless of where any payment instruction comes from or the urgency attached to it.

Prevention – some practical tips

Some practical guidance to help Members avoid falling victim to a scam are included below. Some of these tips originally appeared in our bulletin last year but we have included them again as a reminder:

- Your business may have software, for example a form of e-mail impersonation assessment service. Flag messages such as “reply to address is different to sender” should not be ignored.
- It can be too easy to rely on electronic communication alone. When verifying banking details we recommend procedures require a verification call to be made. Clients will be used to receiving verification calls and will be happy that you are ensuring their monies are protected! Calls should be made using contact details that have been independently obtained. These may be from a known contact or from a legitimate company website. Do not use details contained in e-mails or links from those e-mails. Consider having a particular code word or a method of proving a contact is legitimate. One approach is to ask a series of questions which only the legitimate contact would know the answer to. When obtaining verification, be especially vigilant if anyone avoids answering calls and repeatedly reverts by e-mail.
- Remember, confirmation of bank details provided on a firm’s headed paper is not fool proof; these can easily be replicated, copied and signed, particularly now most transmission is electronic.
- Trust your instincts if an instruction seems suspicious and be alive to typos, random capitalisation and unusual remarks.
- Make sure staff undertake regular cybercrime prevention training.
- Account handlers (including directors/partners) should be informed that the Finance Team is fully authorised to refuse transfers, until the firm’s procedures have been complied with. There should be a consensus between account handlers and support staff that verification procedures must be robustly followed, and that these should never be circumvented due to external or internal pressures.
- Ensure only approved staff can authorise transfers, with all large payments over a fixed value to be authorised by experienced and senior personnel e.g. Finance Director/Deputy Finance Director. Evidence of the payment verification steps should be made available to these individuals as part of the payment process.
- Whilst fraudsters won’t always use overseas accounts, do be vigilant if asked to transfer to jurisdictions with no obvious relevance to the client or the transaction or to a country known to be high risk.

- Be alert to any message or instruction that seeks to create a sense of urgency and insists that you must act now. The aim is to pressurise the recipient into acting with little further thought.
- Notify the FCA, not least so that if appropriate the FCA can update its 'Protect Yourself From Scams' page.

In our previous bulletin we talked about fraudsters deliberately seek to exploit the fact that firms may be handling large sums of client money and operating under huge pressures. We mentioned that busy people may sometimes struggle to cope and may also for example, have domestic worries that are not immediately apparent to others. All of this can impact on someone's ability to spot and prevent frauds. With the impact of COVID-19 and the sudden shift to remote working for many, this holds true even more now than it did then. Whilst many people will be coping very well with the new working arrangements in place during the pandemic, there will be others who are finding things more of a struggle. Firms need to be supportive where this may be the case and to engage proactively, as many are already doing, with mental health and wellbeing initiatives.

Managers: Griffin Managers
Regis House
45 King William Street
London EC4R 9AN
Telephone 020 7407 3588
Email griffin@tindallriley.com
www.griffin-insurance.co.uk

First Issued: November 2020