Stay safe

Robert Rutherford and Nigel Smith outline how to protect both firms and clients from scam e-mails during conveyancing

Robert Rutherford is CEO of business and technical consultancy QuoStar and Nigel Smith is the managing partner of Ellis Jones Solicitors

'The Solicitors Regulation Authority ultimately takes the view that firms are responsible for safeguarding client funds, and in turn law firms must replace any money that is "improperly withheld or withdrawn from a client account".'

The rise in targeted e-mail attacks against solicitors and their clients continues to dominate the headlines, with one couple recently losing a £45,000 deposit after succumbing to an e-mail from a hacker claiming to be their solicitor. These attacks are clearly dangerous in their current form, but the increased frequency and intelligence behind the attacks means that solicitors will need to become increasingly vigilant in this area, not only for their clients, but for the sake of their reputation as well.

The premise of these attacks is quite simple: when purchasing a home, significant sums of money are normally transferred from the buyer to their solicitor, before being transferred once again to the seller of the property. In order to gain access to this money, the hacker e-mails the client from an e-mail address that appears reliable to request the payment transfer at the same time as a property is due to exchange. The bank details included in this e-mail are in fact fraudulent, therefore allowing the scammer access to the client's money.

Attacks can take place from one of two angles here: either the property buyer is targeted, or one of the acting firms. In the first instance, a criminal will e-mail the buyers, claiming to be their solicitor, to inform them that the property is ready to exchange and ask them to transfer the purchase funds to the solicitor's bank account, which actually belongs to the fraudster.

Another approach is for criminals to intercept an e-mail trail, where individuals selling their property have sent their bank account details to their solicitor, in order for the sale proceeds to be transferred to them. The attacker will then pretend to be the seller on this occasion, and e-mail the solicitor's firm, changing the bank details to their own in order to access the sales proceeds. In either scenario, what is clear is that e-mail is the key method for criminals to gain access to these funds.

Why are solicitors and their clients being targeted?

Many law firms continue to rely on e-mail to share the firm's bank account details during a property exchange, but this approach leaves both parties extremely vulnerable to hackers. Criminals have realised that solicitors are the 'middle man' in the conveyancing process, with the potential for huge sums of money changing hands each day.

Law firms have always been a prime target for e-mail attackers due to these ongoing monetary transfers. These attacks show a concerted effort to merge online and offline methods of extracting funds from a solicitors' firm. In some extreme cases, attackers have actually visited law offices in person to gain further information about a firm. By their very nature, these attacks are not conducted at random, but are aimed specifically at a particular firm.

Where should firms begin?

Firms need to devise internal controls and systems that dictate not only when but how staff can securely release confidential

information, financial details and funds. Security basics such as spam filters, anti-virus software and firewalls are already a given as being part of a firm's arsenal against these attacks, so implementing further security processes will only serve to strengthen the fight against fraud.

To combat the threat of these e-mails, it is crucial for solicitors to utilise more secure methods for sharing sensitive and confidential information with their clients. E-mail encryption technologies, password-protected documents and electronic signatures are all relatively simple and cost-effective ways to reduce the level of risk quickly.

Creating a secure, online portal is another effective way of sharing information between solicitors and their clients. Implementing all of these solutions at once is likely to feel overwhelming, but following just one or two of these steps will help to ensure that only the right people have access to the right information, whether that is the firm's data or that of a client.

Many law firms continue to rely on e-mail to share the firm's bank account details during a property exchange, but this approach leaves both parties extremely vulnerable to hackers.

Firms need to be aware of the dangers of using e-mail as a route to transfer sensitive data, and to continuously advise clients on the risks of cyber crime. Clients should be told from the beginning of the process that bank details will never be sent or accepted via e-mail.

If a client does receive an e-mail of this nature, they should be advised not to transfer any money until they have made contact over the telephone to verify the validity of the message. Encrypted e-mails and secure portals are increasingly the solution here. Unless these are in place, face-to-face or telephone validity checks remain the short-term answer, ironically offering an analogue solution to a digital problem.

Solicitors are also increasingly utilising their e-mail signatures as a method of reminding clients about the risk of scam e-mails. While it is by no means a universal trend, security notices of this kind are being implemented by firms to warn clients against taking any

action when receiving an e-mail asking for bank details or to transfer money.

Are there any repercussions for firms whose clients have lost money in this way?

The Solicitors Regulation Authority (SRA) ultimately takes the view that firms are responsible for safeguarding client funds, and in turn law firms must replace any money that is 'improperly withheld or withdrawn from a client account'. As a result, member firms could be left to foot the bill should their client fall victim to one of these attacks. It is therefore imperative that firms dealing with property exchanges take immediate action to warn their clients of the possibility of these attacks.

If a firm can demonstrate that it has robust systems and processes in place that are 'fit for purpose' – and these have been explained clearly to the client – it is unlikely to be found liable in the case of a cyber breach that is not down to its systems. Conversely, if a firm does not have the appropriate systems in place, then it is likely to be found negligent and the client will have to be reimbursed by the firm's insurers. In this scenario, there would inevitably be issues from the SRA, which could involve anything from a fine to, in a really serious case, a firm being closed down.

Unfortunately for the client, however, banks will not readily put up their hands in this scenario, so it is vital to reiterate the message continuously to clients to proceed with caution when sending any money electronically. Otherwise the client could still end up losing their lifetime savings if the insurers can argue that the solicitor was not liable.

Can a firm implement further technology to avoid these attacks?

When discussing IT security, conversations tend to centre on the threat to a firm's assets. An asset can be a computer, a server or even a member of staff. In addition to protecting these assets, firms can start by investing in encrypted e-mails and secure online portals, but should also look into other technological options to add to their security armoury.

Law firms can consider implementing the ISO 27001 standard, which will assist in helping a firm to manage the security of its assets, including financial information, intellectual property, employee details and confidential third-party data, such as that of a client. ISO 27001 uses a top-down, risk-based approach to conduct a risk assessment, manage identified risks and select controls to be implemented across a firm's IT systems. It is a vital first step for a firm that wants to focus on improving revenue and profit, rather than facing concerns over its security. The process is not difficult, and certification can normally be achieved for a reasonable price.

This standard is without a doubt the best way for a firm's leadership to understand at the top level what the biggest security risks are, and the likelihood of an attack, in addition to the impact that a cyber breach could have on the firm.

What about a firm's staff?

A firm's greatest weakness, and therefore requiring its greatest protection, lies within the people it employs. Training will be required for everyone in a firm, from support staff to trainees to managing partners. Anyone who opens an e-mail or takes a call should have received training in how easy it can be to succumb to an attack. In this way, firms can help to sharpen their defences dramatically. Solicitors will be on the right track if their employees are well-trained in this area and continuously updated on the potential for any new security threats. Scam e-mails of this nature are not necessarily sophisticated and can often target more junior members of staff, due to their inexperience in knowing what to look out for. Ensuring that every member of staff is aware of the risks and receives regular training and communication on the latest scams is therefore crucial. In addition, firms should focus on creating a culture in which everyone in the organisation is prepared to question or be challenged over unusual requests and transactions, so that all members of a firm will be fully prepared in the event that they are faced with a scam e-mail.

A firm's greatest weakness, and therefore requiring its greatest protection, lies within the people it employs. Training will be required for everyone in a firm, from support staff to trainees to managing partners.

Training staff on IT security is also key since the human factor will always be a firm's weakest link. It is imperative that shortcuts are not taken here; staff must be taken into seminar-based training and have the risks explained to them. Utilising real-world examples will help to reinforce the training – talk and text will not be enough here. Employees must understand that the whole firm is in this together, with a duty to protect the firm's interests as well as that of the clients.

Falling victim to any type of scam e-mail can be disastrous for a firm, not only from the perspective of protecting a hard-won reputation, but also in terms of protecting its employees and clients from the repercussions of an attack. Whether the firm is at fault or not, any attack on client money will ultimately have an effect on its reputation. Therefore, it is all the more important to invest in robust procedures and IT infrastructures to mitigate the risk of these attacks. ■