GETTING BACK TO SECURITY BASICS

Ellen Freedman, CLM

The Alabama State Bar issued a scam alert to its members on December 1, 2016 regarding a costly email scam. A closing attorney received a last minute email with instructions to wire proceeds from a closed sale, rather than mail a check to the out-of-state sellers, as previously instructed. The email contained sufficient information to convince the law firm it was legitimate, and the money was lost. It was the fact that the email contained sufficient information about the transaction to lead investigators to believe that the scammers had gained access to the email account of one of the parties to the sale, or one of the real estate agents. It doesn't appear that the firm's email server was hacked, but that's still a possibility. An investigation is on-gong.

The District of Columbia Bar has a similar occurrence a couple of years ago. In that case, the lawyer's email was hacked; providing all the information to perpetrate the fraud. The attorney received a last-minute email changing the destination of the closing money. The amount at stake was $150,000. In this case the lawyer was suspicious about the last minute change, so he stopped to call and verify the change. The email was confirmed to be fraudulent, and the ensuing investigation revealed that the email server had been hacked.

On November 1, 2016, the Florida Bar News posted an article entitled "*Sophisticated scam targets lawyers and wire transfers*". The opening sentence states "Never trust a last-minute email that changes the original wiring instructions for transferring client funds." In fact, it's been pointed out that real estate brokers frequently have open discussion on social media about sales of properties. It is an easy trail to follow for there for a scammer to interject themselves at the last moment and intercept proceeds.

Freedman Consulting, Inc.
(215) 628-9422

The Florida Bar has a web page devoted to providing resources for bar members to use to protect themselves from fraud and their computers from malware, and is updated frequently with additional resources related to cybersecurity. This isn't just an issue for closing attorneys, as most attorneys in PA know a firm that has suffered a breach, or came uncomfortably close.

For example, a PA firm had a client arrive to execute a release and receive a settlement check. A paralegal handled the final paperwork, and the transaction didn't take more than 15 minutes. About an hour later the actual client arrived looking for their settlement check. A simple case of identity theft left the firm holding the bag for the settlement funds. The settlement check had already been cashed. The paralegal had never asked for a photo ID before completing the transaction.

We are seeing frauds concerning many practice areas. There aren't many which are immune. The FBI refers to these scams as business email compromise (BEC), a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before. It resulted in actual and attempted losses of more than $1 billion to businesses worldwide. Since the beginning of 2015, there has been a 270 percent increase in identified BEC victims. Dollar losses exceed $740 million for U.S. victims alone.

It's time to go back to some security basics. That means checking legitimacy of identity, last minute instructions and changes, and even emails with unexpected attachments from people we know. It means that more attorney oversight is required before information is shared with people via fax or email, even though they seem to know enough about the matter to appear legitimate. It's so nowadays to "spoof" an email identity (appear that the email comes from one party when it really comes from some else) that we can't trust our eyes.

It's unfortunate but true that there is sufficient economic reward for the bad guys to be able to employ the best of the best hackers. They are more willing to do their homework, and patiently wait for their payoff. They are not obvious nowadays with misspellings, clearly phony email addresses, and so forth. Not that these type of low-thought scams don't still abound, it's just that the really good ones aren't obvious at all. They are meant to sneak under your radar screen.

Of course, your best protection comes from simple but well followed procedures including:

- Employee training at all levels within the firm. It is best to do an occasional validation test to see whether people ignore training and continue to indiscriminately click on links and open attachments, or send out responses without validating legitimacy of the requester, and obtaining attorney permission.

- Keep all software up to date. It's not just your virus and malware software which needs to be current. Any software used at the office can provide an opening for the bad guys to enter and bypass your best security.

- Always have a second layer of validation where money is concerned, so that last minute changes to bank account numbers, addresses, or any other instructions are always checked.

- Don't be pressured into completing transactions involving money before the money is actually cleared, and transmittal instructions are validated. That includes contacting the target financial institution for wire transfers to validate the routing and account number personally.

Our reality will only get worse with respect to the risks, and constant vigilance that will be required on the part of every single person in the law firm. Take a few minutes to create a checklist with your minimum required security steps, and to review and update it on a regular basis. Better to get everyone on the same page than to be left holding the bag, and perhaps wind up on the front page of your local paper.

A version of this article originally appeared in the January 2, 2017 issue of the Pennsylvania Bar News.

Freedman Consulting, Inc.
(215) 628-9422