Phishing for Funds in Real Estate Transactions

"What do you mean you're here to pick up your check," the escrow officer says to the seller. "I wired the money yesterday per your email."

"I didn't send you an email yesterday," the seller replies.

Silence.

Panic.

This is an all too familiar story in the 21st Century real estate transaction and it is an example of what happens when a phishing expedition has succeeded. Mirriam-Webster's Dictionary defines phishing as "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." Developed early in the internet age, the process has become prolific. According to the Anti-Phishing Working Group the number of reported phishing attacks in December of 2014 was 62,765, up from 12,845 back in January of 2005.

In the real estate context, the scammers become aware of a real estate transaction and induce a party therein to wire funds to them instead of their intended recipient. It makes sense that real estate has become a target of these scammers as billions of dollars change hands in real estate transactions annually. The scammers know this and they know that the funds are often moving via wire, a form of transfer that results in funds being available for withdrawal almost immediately upon receipt. This is key to the scam because the longer it takes for the money to be available the better the chance that the scam will be discovered and stopped.

Often, it begins by hackers identifying the email accounts of real estate agents and brokers. This is a simple process as real estate agents advertise extensively on the internet such that their email addresses can often be readily obtained.

The scammers then hack into the agent's or broker's email account. While there, they watch the traffic and look for communications directly related to a particular transaction. Through this stealth activity, they can glean the whole story of a real estate transaction, including who the parties are and when they'll be moving money. That movement, and their hopeful diversion thereof, are the goal of the scammers.

As they watch they note details about the transaction that would be unknown to outsiders. Then, when they think they have enough information to be credible, they send emails to one or more parties in the transaction, inserting themselves into the communication chain instead of the intended recipients. This is often done through the creation of fake or spoof email accounts. The real parties then cease to communicate with each other directly. Instead, all communications begin to flow through the hacker who passes on the information to the intended recipients, as filtered by the hackers. In most cases the vast majority of information does flow through to the parties; after all the hackers need everyone to think everything is ok and if the parties speak in another way, like over the phone, the scam could be discovered if data was missing.

The one area where they do make changes, however, is in the area of how money is to be handled. A seller asking for a check becomes a seller asking for a wire or an escrow company's wiring instructions become wiring instructions to the hacker. The parties being unaware of the fraud, they gladly comply with

the instructions provided and the funds get diverted instead of reaching their intended target. Every minute it takes the parties to discover the fraud and notify the banks involved decreases the chance that recovery of some or all of the diverted funds can be recovered. Once removed from the receiving account, it is rare that recovery efforts will be successful, leaving the parties to fight amongst themselves over liability and responsibility for the lost funds.

Well before these precious minutes, all parties can and should take specific, directed actions to avoid such attacks or detect them in process. By so doing, they may never have to feel the panic described above.

First and foremost, setting the expectations of the parties is of paramount importance. The agents and escrow professionals should advise the principals of how communications are going to be handled and that they should be on the lookout for scammers attempting to divert funds.

As the transaction progresses everyone should verify the sender of all communications. Check the email address against your records to ensure that it truly is from the address you have for the sender.

Then, review the document or email carefully. Often the hackers are in foreign countries such that their communications will have grammatical or stylistic errors. If is also common for attachments to be altered, the cutting and pasting being visible upon careful inspection. The timing of emails is often an indicator as well so watch for emails arriving at non-business hours.

Other common signs of a scam are last minute changes. For example, if the seller says they want a check, then the day of closing emails that they've changed their mind and want a wire, this should be a red flag that additional confirmation or verification is warranted.

Confirming with the parties via telephone, using a known number is a great way to minimize the chance of the funds going to the wrong place. The use of secure and/or encrypted emails relative to the transmission of financial information is also a valuable tool in fighting these types of phishing scams. In particular, free emails like hotmail, gmail and yahoo are notoriously unsecure so avoid using them to communicate any details related to a real estate transaction.

Ultimately, the best defense is being cautious and careful about all communications related to a transaction, in particular those related to funds. By so doing, all parties can minimize their chance of losing money to a "phisherman" looking to score big on their deal.

This article was written by Jennifer Felten, Esq. Her law firm, RELAW, APC, provides legal representation and counsel on various forms of real estate transaction and litigation issues for individuals, real estate professionals and escrow companies. She can be reached by phone at (805) 265-1031 or via email at jennifer@relawapc.com. The firm's website is located at www.relawapc.com.