CYBERCRIME AND THE REAL ESTATE TRANSACTION
How Hackers, Fraudsters and Spoofers are Using Your Email Account to Steal Money Right Out From Under Your Nose

Jane A. Rheinheimer
Rheinheimer + Smigliani, APC

We've grown almost numb to news of massive security breaches involving personal information. From Home Depot to Neiman Marcus, most large retailers, universities and healthcare systems have been targets of cyber criminals. The government apparently can't protect itself either. In May, we learned that the US Internal Revenue Service had been hacked, compromising the most personal information of hundreds of thousands of taxpayers. Even more recently we learned that 5.6 million fingerprint records were stolen from the US Office of Personnel Management earlier this year - biometric data which cannot be replaced like a stolen PIN code.

Now, we find cyber thieves reaching into the residential real estate transaction. And more often than not, they are using you, the Realtor©, as their gateway to entry.

This particular flavor of cyber crime has many manifestations, but it typically works something like this: A hacker breaches the email account of a real estate licensee. This isn't difficult to do, unfortunately. Think about how many times a day, and from how many different places, you access the internet to send an email on your business account. Think about all the marketing and advertising materials you have floating around out there that include your email information. Cyber criminals know who's busy listing and selling properties. The more successful your business, the bigger the target you are.

Once the licensee's email account has been compromised, the hacker can hang out, waiting to interject him or herself into a transaction, usually by spoofing. There are all kinds of spoofing but for the sake of simplicity, we'll call a spoofer someone who sends an email pretending to be someone they are not.

As a very simple example, let's say listing agent Suzy Smith is selling a property in a transaction involving a buyers' agent named Tom Jones. Tom's correct email address is tjones@broker.com At some point, Suzy's email account is hacked by a bad guy. Hacker waits around for awhile, monitoring email communication between Suzy and Tom about the specifics of the deal.

When the time is right, hacker sends Suzy an email from a nearly-identical email address, say tjones@brokers.com, using information he has learned about the transaction to make the communication sound legitimate ("Thanks again for your help Suzy and I'm looking forward to seeing you at the property inspection next Wednesday"). In all likelihood, Suzy will from that point on begin communicating with "Spoofer Tom" about the particulars of the transaction, obviously without realizing that the chain of communication has been compromised.

In some cases, the hacker will spoof multiple email accounts within the same transaction. So, for example, you might end up having "Spoofer Tom" communicating with "Real Suzy" and "Spoofer Suzy" communicating with "Real Tom." Often the emails of the principals, the escrow officer, the title officer, the lender, get spoofed as well. The spoofer, of course, monitors all communications ensuring that the emails look legitimate and contain factually correct information. Situation normal, no one gets suspicious.

In some cases, the worst that happens is that a principal's personal information is exposed to a security breach. Increasingly, however, the object of the scam is to divert money from the transaction to a bank account controlled by the bad guys from whence it then promptly disappears. This can come via a request from any of the spoofer personalities involved – the principals, the agents, the lender, etc. Furthermore, the request for a change in deposit or wiring instructions typically doesn't arouse suspicion because the spoofer already knows the intimate details of the real bank account numbers and deposit amounts.

It should be noted that in general the bad guys/gals who are involved in these setups are quite sophisticated. The communications do not typically involve the improper spelling/incorrect grammar associated with those junk emails we all get from the Nigerian prince wanting to deposit $3 million in our bank accounts if only we will give him our account information. The communications look for all the world like the innocuous details of an unremarkable residential real estate transaction. Unremarkable, that is, until the proceeds of the sale, or the downpayment, or the earnest money, go missing.

Another new-ish scam is the hacker/spoofer who claims to be an all-cash buyer. After insinuating him/herself with the real estate licensees and other persons involved in the transaction, the "buyer" requests information to wire purchase funds into the bank. And....boom.

So what can you do to protect your email account from becoming the portal to riches for some criminal mastermind? NAR has very recently promulgated a fraud alert on this topic and they recommend a number of safeguards including:

- Change the user names and passwords on your email accounts frequently;

- Use really good passwords - a combination of letters, numbers and symbols is much harder to crack

- Invest in the best available firewall and anti-virus programs;

- Avoid the transmission of sensitive information via email;

- If you must transmit sensitive information, use encryption software;

- Don't open suspicious-looking emails or click on links you are unsure about;

- Prior to wiring funds, the wirer should attempt to contact the person giving the wiring instructions for a final confirmation using a verified phone number;

- Clean out your email accounts on a regular basis;

- Trust your instincts - if an email looks suspicious, don't open it even if you recognize the sender.

In the event that there is a loss attributed to a security breach or other kind of cyber crime, do you have insurance coverage to protect your business from third-party claims? At the current time, the answer is "probably not" or at least "probably not enough".

Most general liability/business owners policies do not provide coverage for cyber risks. Although the insurance industry is scrambling to catch up/keep up with the new reality of cyber-liability, the lack of available actuarial data makes underwriting these kinds of policies difficult. In order to make your business a more attractive risk for potential insurers, and in order to offer the best possible customer

service to your clients, you would be well-advised to get ahead of the pack in adopting aggressive cyber-risk management strategies and reviewing them frequently.

Jane A. Rheinheimer
Rheinheimer + Smigliani, APC
1230 Columbia Street, Suite 920
San Diego, CA 92101
619.503.1441
jar@rsdapc.com