Don’t Be a Victim of These Common Fraud Schemes

Protect Yourself Against These Common Spoofing Scams With These Tips and Hints

By Jonathan W. Biggs
Vice President and Director of Risk Management and Education
National Investors Title, Raleigh-Durham, North Carolina
Dec. 19, 2016

Fraud continues to be a growing threat to title agents, and technology provides more and more opportunities for fraudsters to perpetrate their schemes. This article examines some of the more common scams in the marketplace today.

First, let's have a refresher on social engineering fraud. This is a fraud scheme in which the fraudster gains information about a transaction and uses this information to gain the confidence of a person involved in a real estate transaction. (The fraudster might possibly intercept an unencrypted email, gain information through social media or search through the trash.) This information, however acquired, is then used to impersonate a person in the transaction and defraud the disbursing party into wiring money to the fraudster instead of the legitimate party. These fraudsters are now using technology to enhance their scheme and trick well-meaning and innocent victims.

Spoofing Legitimate Parties

There are four primary ways to spoof a legitimate person in a transaction; to wit:

1. Spoofed email addresses
2. Spoofed Web links
3. Spoofed fax machines and
4. Spoofed caller IDs

In each instance, the fraudster uses technology to impersonate a legitimate party: a seller, buyer, Realtor, banker or settlement agent, etc. Each type of spoofing is very easily detected if the proper steps are taken and the time is taken to verbally confirm certain sensitive communications, such as wiring instructions.

Spoofed Email Addresses

Many times, the fraudsters made a slight change to the email address to gain your confidence, hoping you would not notice (e.g. using JonTDoe@email.com instead of JonDoe@email.com). This simply required people to notice the different email address (an additional "T" in this example, or some other different addition or deletion). As the word got around, more people were catching this fraud attempt, so the fraudsters have gotten craftier.

Every email address has three ways that it can be viewed:

1. Screen name (e.g. John Doe)
2. Actual address (e.g. JohnDoe@email.com) and
3. IP address (contains a string of four numbers, e.g. JohnDoe@[196.168.0.1] in the address)

One way the fraudsters conceal their true identity is to use the screen name to cover the actual address. If you tried to send an email with the address formatted "John Doe" and not JohnDoe@email.com, it would not go anywhere, but your address book may show the screen name and know what the actual email address is.

If you are sending or receiving an email, if you "hover" over the screen name, you will see the true concealed identity. You will see something that looks like:

> John Doe <IWanna@TakeYourMoney.com>

If you read that you were communicating with someone you did not know (or with someone at TakeYourMoney.com), you certainly would not trust the communication. Additionally, just because the email came in an encrypted format, does not mean it is legitimate. **Always call independently known phone numbers and confirm wiring instructions.**

Spoofed Web Links

The fraudsters will use this same technology to spoof a website. You see this a great deal on phishing emails that are pretending to be someone with whom you do business: an Internet service provider, bank, store or other legitimate business. The email bearing the logo of your bank may say something alarming like:

> “Our fraud investigation team has determined that your account may have been hacked. Please click on the link below to log in and change your password.”

Previously, the link might look like this: http://iaosdngkdis.com or http://MyBank.TakeYourMoney.com. The first one is unrecognizable and should not be clicked, but the second one has the name of “My Bank” in it and you may wonder if it is legitimate. It is not.

Today, they are spoofing the web address, hiding it beneath “Click Here” or by using a legitimate-looking character string and hiding the true destination by saying, “Click Here: My Bank.” You can detect a spoofed web address by hovering over the link to see what truly lies beneath the link. You might see something that looks like this:

> Click Here <http://IAmABadGuy.com/YourBank>

If you need to visit someone's website, verify the URL or type the name of the website into the address bar on your browser.

Spoofed Fax Machines

Some of you have said to yourselves, "I have had enough; I am going back to my fax machine." Once you get it out of the closet, you may have to set it up. The first thing that you will do is put in the "Sender's/Your" number into the memory so it will show up on faxes that you send. Then it hits you: the fraudster can do that, too, thereby impersonating or spoofing the legitimate sender.

Fax machines are still a very useful tool, but remember that the fraudsters know how they work, too. The same thing is true for regular mail. The fraudsters can impersonate legitimate parties just as easily as you can send a letter or a fax.

Again, always call independently known phone numbers and confirm wiring instructions.

Spoofed Caller ID

Fraudsters have taken their deviousness to new lows.

So you have read the alerts and other communications, and you would never send a wire without verbally confirming wiring instructions at a safe, known and independently verified phone number. You are almost ready to send the wire, so you look for a safe contact number.

About that time, you receive a phone call from the fraudster pretending to be the recipient of your wire. You have caller ID, and you check the caller ID on your phone to your safe number in your file. You asked the imposter/fraudster questions about the transaction and they seem to know what they are talking about. Now you feel comfortable. Do not!

Fraudsters and thieves are utilizing prepaid "burner" phones and applications that will spoof the caller ID of any phone number the caller chooses – even valid phone numbers of actual businesses. A pre-paid phone can be purchased at a convenience store and then discarded when the minutes are used. Fraudsters are combining this low-cost phone with a phone application designed to prank your friends; however, they are using this insidious combination to spoof parties into a transaction: Realtors, banks, tax offices – and the list continues to grow.

Fraudsters have quickly learned that our responsible title and settlement professionals have begun utilizing call-back procedures to validate and verify emails regarding wiring of funds. The fraudsters continue to adapt their scheme in an attempt to circumvent our protective practices and procedures by spoofing the caller ID.

Don't get spoofed! An incoming phone call never takes the place of an outgoing confirmatory call before wiring funds.

How can you protect yourself against these scams?

1) Encrypt emails or use other secure methods to deliver any communication containing wiring instructions, details of the transaction or other sensitive financial information (such as a settlement statement).
2) Exercise a high degree of suspicion for any wiring instructions you receive that do not come through encrypted email from a trusted source, especially if they replace existing wiring instructions.
3) Prior to wiring any funds, confirm by telephone that the intended recipient of the funds did in fact send or change its wiring instructions.
4) When confirming by phone, do not rely on phone numbers or web addresses in those emails, as they would be fraudulent as well.
5) Always look closely at an email address prior to hitting "Reply" to see if it is spoofed.
6) Utilize "Whois" lookup services like whois.net to research URLs and confirm details, such as when a domain had been created and to which organization it is registered.
7) Educate parties to the transaction to only use encrypted email or other secure methods to deliver sensitive transaction information. Further educate them that you will only use encrypted or secure technology to communicate with them.
8) Contact your insurance agent about purchasing cyber-fraud insurance. Please make sure that the coverage includes recovery for a cyber-breach (loss of information), cyber-crime (loss of money) and cyber social engineering fraud (as detailed hereinabove).

****

About the Author

Jon Biggs oversees risk management functions related to National Investors Title's approved provider system. In this role, he oversees the approval process, develops educational seminars and communications-based initiatives involving approved providers and agents and manages provider data and analysis related to the company's risk management efforts. Prior to joining National Investors Title in 2012, he was partner at a firm in Durham, North Carolina, where he practiced residential and commercial real estate law for more than 20 years. He holds a bachelor's degree from Duke University and a Juris Doctor from Wake Forest University School of Law.