Straight Talk Title: Email & Wire Fraud Doâ??s and Donâ??ts

Description



VLTA Examiner

I know youâ??ve heard all about it, but has it happened to you? If so you know exactly what Iâ??m talking about. When I tell you, this is the scariest thing Iâ??ve ever seen in our business, I mean I worry everyday about the hidden hack. We canâ??t see where itâ??s coming from or whatâ??s happening to us or our customers until sometimes itâ??s way too late. This all takes place behind the scenes and title companies and their customers are being attacked everyday by people they canâ??t even see or touch. With the simplicity that the internet brings, it also brings lots of room for newer bigger problems.

Have I scared you? I hope so, this is very serious and we need to be proactive for ourselves, our customers, and our Realtor and Lender partners.

Now you may be thinking this will never happen to me or my customers, I can guarantee you it will. No matter how much protection you have, just like any other type of robbery, if a robber wants to get in, they will find a way. Our job is to make it tough so they will give up and move on. I assure you, if you havenâ??t had an intrusion yet it will happen so letâ??s talk processes and protection.

The one place youâ??re most vulnerable is the team member you have sitting in front of the computer. So, you MUST educate them regularly on the changes and new ways hackers are attempting to get in.

Email and Wire Fraud ranges from hackers looking for your account numbers to scammers who want to infiltrate your communications and convince your customers to transfer their funds for closing to them. They want to get into your system, so they can talk to your customers as if they are you and the only way they can do that is to get your customers contact information, so their communication will look as real as possible to your customer.

Letâ??s talk about how they can get into your email first. I am sure youâ??ve seen the warnings about suspicious emails with misspelled words, crazy email addresses or seemingly obvious typos in them. Let me tell you these criminals are getting smarter and their scam emails donâ??t have typos nearly as much anymore so, you must be smarter!

Hereâ??s some steps to take to try to help you stay ahead of the hack:

- First, take your time when reviewing the emails in your inbox.
- Click on the senderâ??s email name or address, this will reveal the email address that is REALLY sending you this email. If youâ??re at all suspicious about the email this will confirm that.
- Donâ??t click on links in email, copy the link and open it in google.
- Encrypt every single email that goes out of your office, itâ??s a very affordable protection for you and your customers.

Now ask yourself before opening or responding to an email in your inbox:

VLTA Examiner

- Do you know the sender personally?
- Are they asking for something they wouldnâ??t normally ask for?
- Are you getting an email from someone that usually calls or texts you?
- Is the email from someone in your office at the desk next to you that would normally turn around and ask a question?
- Is there an unusual sense of urgency in the email? (this is a common trick to get you to act, without taking the necessary time and precaution to review it).

These are all common ways hackers use to trick you into clicking on an email so they can get into your computer. Once they are in, they will watch your emails for information and once they get all the players in a transaction they can send a fraudulent email to your customer to trick them into sending their closing funds to somewhere other than you.

If you have any suspicions about an email, pick up the phone and call the sender but not at the phone number in the email because that is more than likely fraudulent too. Call the sender at a number that you have from another source, the contract, realtor or looking them up online.

You may be thinking, well I am not sending the fraudulent email so how will I be liable? I assure you if someone loses their money to a fraudulent email or text, it doesnâ??t matter what you did, youâ??re in the loop and understandably, the customer will do anything they can to get the money back. Typically, they will include everyone in the transaction in a lawsuit to try to recuperate their lost funds. So, make sure you document everything and do everything you can to protect yourself.

Letâ??s face it, we all want to make sure that closing takes place and if our consumer doesnâ??t have the money to close because they sent the all the money they had to Africa then it wonâ??t close and thatâ??s a problem for us all!

We all know consumers already donâ??t understand most of this process, so we need to educate them, the Realtors and the Lenders. They should all be using encrypted emails and not discussing financial matters over email. Hackers are most easily getting in through free email accounts like Gmail, Yahoo

and Hotmail. More often than not itâ??s the consumerâ??s email or the realtors email that has the vulnerability and is allowing the hacker to gain access to the transactional information. This being said, none of us want our consumers to be robbed and instead want them to go to closing, so letâ??s educate them and ensure their money is safe!

Now that weâ??ve established ways that hackers can get email information on your customers, so they can send fraudulent emails, letâ??s talk about how their scam works to get your customerâ??s closing funds.

A scammer typically gains access to a title companyâ??s or real estate agentâ??s email account and searches for home purchases or refinances scheduled for closing. He will then create a fake email address that closely resembles the real thing, such as john.doe.abctitle@gmail.com. With access to the real email account, the scammer can observe the formatting of previous email exchanges and craft an email that looks very authentic, down to the email signature and company logo. Using this genuine-looking email, heâ??s able to impersonate a representative at the title company handling the transaction and provide fraudulent wiring instructions to the customer that will funnel the closing funds directly into his own bank account. He will ask the customer to confirm when the funds will be sent and he will express extreme urgency in the email so that they consumer will act quickly and not ask to many questions. Once the hacker knows when the funds will be coming he is waiting for the funds to hit his account and will immediately remove the funds so that the wire cannot be called back. Remember a wire transfer is an immediate form of payment. It is almost always irreversible, even if fraud is involved.

VLTA Examiner

Notify your Realtors and customers:

Let them know that they may be a target of a hack if they received notification from an email that looked to be from you that stated:

- Previous wire transfer instructions were incorrect and provides new instructions
- Uses an excuse for sending the wire transfer to a different account.
- For example, one business was told that an escrow account was being audited so the wire needed to be sent to another account.

Instruct your customers of the following:

- Before wiring any funds, always confirm wire instructions with their title company rep by calling a phone number they trust. Do not call a number from an email if you havenâ??t used it before, fraudulent emails often contain fake phone numbers.
- Verify the full email address of the sender. This process will be different for different mail servers. For example, when you open an email you can tap the senderâ??s name to reveal the full email address. If the email address does not end in the company name (meaning you donâ??t see â??@CompanyName.comâ?•), this is a usually a fraudulent email. Note the difference between john.doe.abctitle.com@gmail.com and john.doe@abctitle.com. However, sophisticated scammers can also spoof an email address by making a fraudulent email appear to come from john.doe@abctitle.com, so always confirm final instructions by phone.
- Encourage them to be highly suspicious of any correspondence stating the wiring instructions have changed. Remind them to call you directly if they receive this type of communication.

Finally, if you or any of your customers have spotted a scam before sending the money, please report it, this is the only way we have any chance to try and stop these things from happening, hereâ??s how to and who to report it to:

Report the incident to the Federal Trade Commission and the FBIâ??s Internet Crime Complaint Center as soon as possible and provide all of the incident details. If your bank asks for a police report, give them a copy of your report to the FBI.

Call your local police department financial crimes division and file a complaint. They canâ??t do much without a loss but protect yourself by being proactive.

According to the FBI, nearly $1 billion was diverted or attempted to be diverted from real estate purchase transactions and wired to fraudulent accounts in 2017, letâ??s not let our customers be one of these losses in 2018!

For more information like this or to download our freebie, â??7 tips to launching your first live

heck out www.conniefuksa.com.

VLTA Examiner

Connie Fuksa is an energetic speaker and facilitator and author who is on a mission to raise awareness of the value and purpose of title agencies and the intricacies of the title/closing process so that consumers can make more informed buying decisions. As the head of her own title company for nearly 30 years, Connie knows the challenges of the title industry, but also sees the opportunities. She is pioneering a new way of doing business by empowering title companies to grow passionate teams and better communicate with consumers. Connie also produces a regular broadcast that provides advice and home closing information directly to consumers. Outside of her work, Connie loves to ride her Harley and loves being outside and gardening. Sheâ??s been married for over 27 years and is proud momma to a son whoâ??s a Navy sailor and a very active pup.

Category

1. Cybersecurity

Date Created
2018/06/05
Author
vltaexaminer