**How to Educate Clients About Real Estate Scams**

[00:00:00] **TRACEY HAWKINS:** Cybercrime, cybersecurity, and fraud. Knowing how to avoid falling victim to those things is an important way to show your value to your clients. But how do you have those necessary conversations to protect yourselves and your clients? What do agents need to be aware of as you conduct your transactions?

You're listening to Drive With NAR: The Safety Series—powered by REALTOR® Magazine in partnership with the REALTOR® Safety Program. Hear harrowing stories from real estate pros who have faced danger in the field and expert advice on how to work safely. Get more real estate safety tips at nar.realtor/safety.

I'm Tracey Hawkins, and I'm here today to share best practices with two real estate pros, tips that can help equip you and your customers with information to stay a step ahead of fraudsters.

First up is Heather Ozur, a real estate professional with more than 25 years of experience. She specializes in residential properties in the greater Palm Springs and greater San Diego areas of California. She currently serves as the 2024 President-elect for the California Association of Realtors®.

Hi, Heather.

[00:01:12] **HEATHER OZUR:** Hi, great to be here. Thanks, Tracey.

[00:01:14] **TRACEY HAWKINS:** Next we have Nicholas Lagos. He's a real estate professional based in Northern Virginia. He was the past president of Northern Virginia Association of Realtors® and currently serves as NAR's chair of the Risk Management Committee and the Board of Directors of Virginia Association of Realtors®.

Hi, Nick. Thank you so much for joining us.

[00:01:33] **NICHOLAS LAGOS:** Thank you for having me, Tracey.

[00:01:34] **TRACEY HAWKINS:** First question I have for you is experience. Have either of you all experienced any kind of a transaction where there was a scam or fraud?

[00:01:44] **HEATHER OZUR:** I've had clients have experienced the emails and notifications from whether it be escrow or title that seemed a little shady, and I'm thankful for the conversations that I had with my clients ahead of time when we started the transactions to understand to watch out for this and to not fall victim to it.

So, luckily so far, my clients have not fallen victim to it, but it's because clear, concise conversations and really making them realize that they have to be due diligent in this themselves and be cautious.

[00:02:16] **TRACEY HAWKINS:** Heather, give me an example. Do you have a real-life story that you can think of where either a client received the email and they questioned you about it?

[00:02:25] **HEATHER OZUR:** I've had clients just this year, they received an email that they felt that didn't seem right and they questioned it. They called me right away, screenshot the email, and said, “Is this from escrow? Why would they have contacted me this way?” And so again, went over the conversation of that, “Probably this is not from escrow. Escrow was clearly explained to us that this is not how they were going to contact you throughout the transaction.” And we called escrow together and asked what they were looking for and was this from them, and which they shared to us that it wasn't. So again, it was just having my clients prepared that something like this could happen.

So it sounds like you had a conversation right up front, letting them know that there are certain things that they need to watch out for. Do you remember what specifically was the content of the email that raised the flag?

What raised the flag is it was a text, and escrow doesn't send text to my client.

So it was that type of flag that was raised. And so it was how the communication came across. It wasn't the normal way escrow communicated with the client throughout the transaction.

Excellent point. So that means you had a conversation and you told them, “Beware of text.” So good job there.

Nicholas, what about you? Can you share a story of a cybercrime or situation that you've experienced?

[00:03:33] **NICHOLAS LAGOS:** Well, we've experienced it in a number of different areas, both in the rental scams, property scams, the wire fraud through title companies I work with, and also impersonating sellers or buyers of transactions. But in particular, a recent one is a client who was moving into this area, who ended up becoming a client only because he sought out my services. And he had applied for a property thinking that the property was a legitimate property, but the person who was renting the property was not. They ended up losing nearly $6,000, both for the first month's rent and the security deposit, because when they came into the Northern Virginia area to move into the property, that property was not even for rent.

So, it did cost them a substantial amount of money and then they sought out my services.

[00:04:22] **TRACEY HAWKINS:** In my training, I talk a little bit about what to look for. Now, as you mentioned, a lot of times the criminals can hijack a listing. So even without the agent knowing, without the seller knowing, they take over the listing and they advertise it to be their own. And what typically is a red flag is if the price is significantly cheaper than what it typically would go for on the market. So in that situation, buyers get excited and they wire the money.

Nowadays, agents are tasked with showing your value. Here's where you add value with safety. A part of your conversation needs to be advising the buyer that this is a possibility, that when you're looking at properties, if you see something, please start with me, your real estate agent, and let me check it out and make sure it is a legitimate and a real property.

Heather, you mentioned having that consultation with your buyers. What are the conversations that you're having? How are you outlining to them what they need to look out for and how they can utilize you and your experience?

[00:05:21] **HEATHER OZUR:** So when I do my buyer's consultation, this is one of the steps that we talk about is the importance of the communications that we have between me and the client, as well as as we continue further with the transaction and get an accepted offer between the lender, the escrow company, the title company. So anybody that's involved. So we have clear conversations about what to expect, how we will all communicate, and especially when it comes to wiring money, how that will come a place.

Here in California, we use escrow is the third party that manages the transaction once an offer is accepted. So I clearly explain to them how they are going to receive communication from the escrow company and that how there is authentication from the escrow companies regarding getting communication to them. How they will clearly, especially when it comes to the wiring of funds, that they actually have to call into escrow themselves to get the account numbers.

And I again, make it very clear that escrow is not going to communicate with you via a text message. It's all going to be via email and from the escrow office directly, but most importantly, how, and when they send the wire instructions of how that will come from the company.

[00:06:30] **TRACEY HAWKINS:** And that underlines the importance of real estate agents sharing the proper communications the checklist. And this is what I say: agents, you need to talk to the sellers as well as buyers and you need to say here is a list of the proper communication, um manners, who you're going to talk to, here is my email, here is my phone number, here's the escrow company, here's the title company, lender. All of that information needs to be on a sheet of paper that you provide to them. That way there's no guessing or second-guessing who it is that they contact and um, if they get an email then they know to double-check that list. So that's another value add for you.

Now Nicholas, I know that you are um on the or you lead the Risk Management Committee. Talk to us a little bit more about business email compromise. How are you talking to your buyers about emails and safety practices using emails?

[00:07:23] **NICHOLAS LAGOS:** Well, very much like Heather, I provide to them a sheet of what to look for, what not to look for.

In addition to the sheet, we have a consultation. I rarely, if at all, work with a buyer or a seller unless I've had a conversation or a meeting in person. Once that happens, I let them know that for me, they are to use two separate email addresses and they are to copy both email addresses. Therefore, they know they are coming for both of me, my email addresses, and that I am copied on both.

So, if they do not get a response from me directly, then they know that there's something wrong. And by using the two email addresses, I'm able to be assured that I'm going to receive that email to make sure that happens. I also let them know that not to share any personal information (bank accounts, social security numbers, tax ID numbers, driver's licenses) over an email or over a text.

It is very important that safeguarding that data is very, very critical. When I am working on a sales, very much like Heather mentioned, The title companies have specific instructions how they are going to be receiving funds. Those are safe encrypted funds that they will get. They will never accept it over the phone and they must use the dedicated secure line.

When we're talking about rental transactions, we've actually built a portal and we use bank-encrypted technology when we ended up getting those communications and monies from those people. Therefore we are sure that that is coming only from us.

[00:09:01] **TRACEY HAWKINS:** Explain the two email addresses and how that plays into the safety and security practice.

[00:09:07] **NICHOLAS LAGOS:** For me, it's mostly assurance that when they get an email from me, they will get an email with my second email copied. It's very easy for someone to hijack an email. You can go on a webpage, for example, and be able to get people's names and addresses and email addresses. That doesn't necessarily mean that the company has full control over that, because as real estate agents we have all of our information out there. It's exposed and we're exposed, and the cyber-attacks are one or two steps ahead of us. We're trying to catch up to them and we need to be diligent. By providing two email addresses they at least know that that email is copied, my second email is copied, and my second email is not published, so I'm only using it for people that I have to work with.

And also my second email, that they know if I send a document, that second email is copied, so if they only get one, they've been instructed to call me to make sure that if I'm not copied on the second email to call me to make sure that I didn't accidentally make a mistake, forgot to include it, to make sure it came from me.

[00:10:16] **TRACEY HAWKINS:** Okay, that's a great approach. I've not heard that before. Okay, before we move on, let's just put a button on the email issue. Free emails are a secure risk. And for that reason, it is advised that real estate agents and brokerages not use free email accounts. I always advise that real estate agents should be using your company's domain email.

Cybercriminals see email, free email accounts, they get excited because like you said, Nicholas, those are the easiest to hack. But when they see a domain email with your real estate company name, they know that that real estate company has strong security protocols and those are less likely to be hacked.

And I always say that brokerage and leadership, you should make sure that your agents are using your email accounts because if their personal email accounts get hacked and the consumer sues, guess who they're coming for?

Let's talk a little bit about that consultation. We need to talk about how to make sure that the client is who they say they are.

[00:11:12] **HEATHER OZUR:** As I've done for years, which is having the in-person or via zoom, uh, as times have changed, uh, buyer consultation with my clients, I do that so I can see them and look at them face to face and have a real conversation versus having something over the phone and not being able to see my clients. I ensure that I'm able to check who they are, who they say they are.

I don't work with a random buyer that, which we get lots nowadays of investors that want to text me and say, “do you have something off market? You know, i'll work with you directly if you have something.” I don't work with clients like that. I work with a client that's choosing to meet with me, spend the time to have that consultation so we can clearly talk about all the various steps throughout the transaction, the safety issues that can be involved, the protocols that can be involved, and how we continue move moving forward as a team together.

[00:12:01] **TRACEY HAWKINS:** Let's talk a little bit about land scams.

What about you, Nicholas, any stories to share?

[00:12:06] **NICHOLAS LAGOS:** We had a person that wanted to list a lot. It was not a large piece of property. They were very anxious to sell this piece of property, they had all the credentials, all the information, but we had not met this person directly. Ended up doing a little bit of research, had the title company do a little bit of research, come to find out that the person who was calling us was not even the owner.

It was actually a subsidiary of the owner. They wanted to impersonate that owner because that owner was overseas. It was very easy to say that they were the owner because it was very, it was a little harder to verify that information. Fortunately, none of my clients have gotten caught by that, but it has happened, and that they are really not the seller who they say they are.

[00:12:52] **TRACEY HAWKINS:** NAR has a *Window to the Law* video series, and if you were to look on the website, you will see a *Window to the Law* that addresses this topic exactly, and it talks about avoiding vacant land scams. Let me just list a couple of the tips that are on there. A red flag is if they list it for significantly cheaper than it should be, if they prefer cash, if they do not want a for sale sign, and if there's an urgency to sell it quickly, and they never meet in person, and typically you'll find that the client is out of state, and they only want to use a remote notary.

So Nicholas, what would you say to your fellow agents as, uh, what they need to do to make sure that they are not the victims of a land scam listing?

[00:13:38] **NICHOLAS LAGOS:** Do your homework, do the research. As real estate agents, we have a wealth of information available to us, not just through our multiple listing service, but through our title companies, our affiliates, and our common sense.

[00:13:53] **HEATHER OZUR:** We need to do our due diligence to confirm who the owner is, reaching out to the listing agent and finding out that information, making sure all that information is available matches. As a real estate agent, we really have to take the time to slow down and have conversations. If it's too good to be true, it probably is. So if the price is really aggressive and we know that everything else is selling at a significantly higher price, well, what's going on? Why is this one piece of land so significantly reduced compared to everything else?

And so again, having those conversations regarding the whole aspect of watching out to make sure that their interest is being put forward.

[00:14:34] **TRACEY HAWKINS:** Right. And again, showing your value, talking to sellers, or in this case, people who own land. So if you live in an area where there's a lot of land, as a real estate agent, there's no harm in reaching out to, um, landowners, and this is business development/safety, and tell them, you know, there are land scams here and I just want to make sure you're not a victim, so here's what I advise you to do. Um, check on your property on a regular basis. If it's a house, make it look occupied. If it's land, keep it mowed and updated.

We'd like to thank FOREWARN for sponsoring this episode. The FOREWARN app provides instant identity verification and risk assessment of prospects with as little as an incoming phone number, enabling safer engagements and smarter interactions.Visit www.forwarn.com to learn how to combat fraud, mitigate risk, and stay safe with FOREWARN.

I cannot have a conversation about cybercrime without talking about generative AI's role in cybercrime.

Nicholas, we talked about how if someone sees a property listed and they're using that as bait, pretty much. Think about nowadays. Instead of hijacking an existing listing, cybercriminals are using these tools to create listings, listing pictures of every room of the property. They're making it desirable. And then they're posting those on either Craigslist or Facebook. So, there's another conversation that needs to be had with the consumer about the risk involved in generative AI.

[00:16:04] **NICHOLAS LAGOS:** Taking all the proper steps is so critical, and that's mostly data driven. Protect your data, follow your data, do your research. And this is where as real estate agents, where we have to show our value. Keep in mind, when we take a listing, we will not only do some due diligence on our own, But we are required to have our partners help us with that, whether it's a title company or a lender or persons that referred it to us.

That's why, and Heather and I both touch on this, you need to be able to speak to the people first face to face. You need to know who they are. The title companies right now are starting to not only get wise to it, but they're also being very proactive. The week before last, I did a transaction of someone that I've known for 25 years.

And for the first time ever, I was called by their attorney and asked, do you know this person? How long have you known this person? Where have you worked with them before? I was able to answer those questions in the affirmative. But even then they said, “We do require two forms of the ID when they come in.” No longer just you show up and you put a mirror to your face and you have a fog. Um, you know, you need to be able to know you, who you are working with.

[00:17:26] **TRACEY HAWKINS:** Speaking of the tools, Heather, one way the cyber criminals are using those tools is they're writing phishing emails, and these are wire change instruction emails that are now grammatically correct.

In the past, they were so poorly written, and that was red flag number one. So there has to be a conversation with the consumer about the emails that are going to come that look legitimate. What is your conversation with your consumer regarding AI and those phishing emails?

[00:17:54] **HEATHER OZUR:** We talk about the fact that they could receive emails that look a hundred percent professional, look like they're coming from the correct place.

I advise them first off, check the email address it's coming from. Usually that's a clear giveaway because escrow, you know, or anybody, we have a set email address. These are the email addresses that we provided to you and the domains in which they're coming from. But again, do not respond to the email if you don't feel comfortable. Call me, take a picture of it, we'll discuss it. We can reach out, make a phone call, have real conversations with real people regarding this, not the numbers on the email that you get, but the numbers that I have provided you of how to get in contact with escrow and title.

[00:18:32] **TRACEY HAWKINS:** Before we wrap, my final question is technology.

You've heard it said that agents who use technology will replace those who are not using technology. So let's talk a little bit about the technology that you are using, especially to detect these AI scams or any other scam.

Nicholas, what's in your toolbox?

[00:18:50] **NICHOLAS LAGOS:** We use two-factor authentication in most of ours. I do use the FOREWARN, mostly for identity, who I'm working with. Change your passwords frequently. I cannot stress that enough. There are many agents and consumers that are using the same password for just about everything you could imagine. That is one of the worst things you can possibly do. Communicate very clearly with your clients and your office. And be diligent. If it doesn't look right, if it doesn't sound right, if it just gives you a gut feeling something is wrong, then you need to do your due diligence and look into it further.

[00:19:30] **TRACEY HAWKINS:** Two excellent points. First, you said passwords. What's even better is a passphrase or even a passkey. A passphrase would be two unrelated words, so two random words as a password, or even a full sentence. And then a passkey is using AI biometrics. So that could be a thumbprint, it could be face ID. Those are almost impossible to bypass.

And by using two-factor authentication, you can reduce your crime and make it where 99 percent of the time you are not a victim. When we talk about passwords, 80 percent of the crimes involving passwords include hacking those passwords. So the harder you make it, the better.

Heather, what is your conversation or basically what's in your tech toolbox to prevent cybercrime?

[00:20:12] **HEATHER OZUR:** Personally, for me, I use a password scramble type of app. So I use 1Password, I've used it for years. So I recommend it to clients when I talk to them about things like that.

Recently, I had a close friend just on Facebook, lose access to their entire account because someone hacked their Facebook account, now sending out information that they're involved with Bitcoin and that they're selling Bitcoin and how they can do it. But they mask it as though they're still the real estate agent. They're still the real person and implying that, but it took a bunch of us clearly sharing with Facebook that this is not the real person and this account has been hacked. It's not easy. Once it, once it happens to people, it's a really tough go around to try and pull all that information back.

[00:20:54] **TRACEY HAWKINS:** Exactly. And it is going to cost you a lot of money if you don't invest in cybersecurity practices, as well as education upfront. And your reputation, as we talked about, is almost impossible to get back.

Keeping in mind that NAR does not endorse any tool or service, thank you for mentioning the one that you use. And may I also suggest that any kind of password locker is a good idea. If they don't have a backup plan in place, they're out of business.

Now we're going to wrap up with a call to action for your fellow real estate professionals. I'm going to ask each of you to tell me what action item you are challenging your fellow real estate agents to use going forward to make sure that they are showing their value, protecting not only themselves as they work, but their data and the consumer.

[00:21:38] **NICHOLAS LAGOS:** My two things would be number one, to put your proposition in writing, which includes your protection for your data include, and protection for them.

My second one is to tell agents and consumers, please do not keep your computer open in the sense that you're just auto logging in, you push the button and it logs you in. Go the extra step, log in your password, because it's very easy for someone to come in and hack into your computer and your data is wide open there.

Not only have you opened your data to whoever's perpetrating it, but you But you've also opened to everyone else who's connected to you. So the bottom line is, show your value, but show your due diligence in terms of password protection and data protection.

[00:22:22] **TRACEY HAWKINS:** I like that you're talking about protecting your devices. Having that PIN or password, not only on your laptop, but your device, your cell phone. Because if it's lost, if they don't have that PIN, then it's just an expensive paperweight.

Heather, what is your call to action for your fellow real estate professionals to protect themselves and their clients and to show that value proposition?

[00:22:42] **HEATHER OZUR:** It's really important to have that in-person or via Zoom type of interview with your clients, whether it's seller or buyer. Life has changed. So virtual is okay, but you still need to see them. Everybody needs to be on camera. We need to have this face-to-face conversation of knowing who each other is. Asking the sellers, and the buyers at times, I ask them to share their driver's license, things like that. I need to know who you are for my own safety, that you really are who you are. So it's, again, it's conversations, walking them down a clear checklist of things that can come across them that are incorrect. And here's how you're going to check out to make sure that these things are correct.

[00:23:20] **TRACEY HAWKINS:** And not to throw too big of a wrench in that, be sure that that video consultation is not a deep fake. Do your extra due diligence to make sure, like you said, who you're talking to is actually who you're talking to.

Now, my call to action will be no surprise: education. Everyone needs to take the time to educate yourself on the types of crimes, especially cybercrimes, that are only growing, um, not only to protect yourself and your data, to protect the industry. Customers and clients need to know that we are looking out for them. So take that cybersecurity class, invest in the tools that you need in order to stay safe. And everybody remember your value proposition is keeping the consumer and the industry safe.

Now stay safe.

Thank you for joining us on Drive With NAR: The Safety Series. New episodes of the Drive With NAR podcast drop twice a month at magazine.realtor/drive or wherever you get your podcast.

NAR does not endorse any product and does not take a stance on any specific safety tool. Members are encouraged to use only those safety tools in which they're properly trained. Find more safety resources at nar.realtor/safety.