**NAR Episode 10 Final Transcript
Guests: Randy Hatada and Bill Soffel**

**Intro**: You're listening to Drive with NAR powered by REALTOR® Magazine. Listen in as real estate pros talk tools of the trade and share stories of inspiration. Get ready to step up your business. This episode is sponsored by NAR Travel Club, the travel booking platform with savings exclusively for NAR members. The following is a conversation moderated by Janelle Brevard.

**Janelle Brevard**: Today, we're going to talk about the important issue that literally affects every member's business. And that's cybersecurity. How can REALTORS® stay safe online? And what are some of the real-life threats that agents are facing? We're going to talk about all of that today. Joining me is Randy Hatada. Randy is broker/owner of Xpand Realty in Las Vegas. We're also excited to welcome Bill Soffel, and Bill is broker/owner of ERA Team VP Real Estate in Chautauqua, New York. This is an important issue. I'm so excited to talk about it. So let's just jump right in. So both of you have experienced cybersecurity threats to your businesses in various ways. I'd love to hear about your experiences. Randy, can you start for us?

**Randy Hatada**: We've been, I guess, a victim to multiple cyber crimes. And I'll start with the common one, which is potential wire fraud. And in the past, we've had our, first of all, our emails are on a Gmail based platform, and it goes under our company name, doing some discovery. And all of the above, I found that Gmail is one of the most popularly used and targeted email platforms, you know, in the nation. So, you know, it is very critical that we are aware of that. Based on that, we had multiple hackers that have breached our emails for multiple agents, including myself, we've actually luckily caught three, three hackers that have breached the system on three different occasions. And they stayed anonymous, where they would intercept emails for them on as if they weren't there. And they were looking for wires. And when they received a wire, and this was back, three, four or five years ago, when we didn't have as much protocols for wire fraud. They would then replace the wire instructions or instructions. And I guess asked for the monies to be forwarded somewhere else. Luckily, we found the error and caught, caught that or stop that from happening and took another route. But had that gone through this would be another conversation. And again, they've reached three different agents, three different emails in three different attempts. The most current issue that I'm dealing with is I am actually under ransom for our phone number of 13 years for Xpand Realty. And during our time, using this number as Xpand Realty. Seven years ago, our IT company switched providers in order to up our technology and our phone lines for the VoIP systems. And the new company that took over the VoIP services. Basically, after seven years, they decided to hold our phone number hostage in in exchange for a specific dollar amount and my driver's license of which I would not adhere to. So that's kind of what we're dealing with right now.

**Janelle**: That's something Randy, I am just like, I don't even have the words for how crazy that absolutely sounds. Bill. Have you had a similar situation?

**Bill Soffel**: Well, yes, you know, we've had similar experiences, we've only really had to deal with one significant problem. We do use Microsoft Outlook Exchange, not Gmail, even so we periodically receive emails that appear to be bogus. And we're certainly more aware of how to pick those up. Now, Randy said, you know, three to five years ago, I think we were all trying to catch up and learn how to navigate this space. But a separate issue, of course, is that our agents, in many cases use their own private email outside of our Microsoft System. So in some of those are Gmail, some of those are Yahoo, et cetera. So there's quite a bit of vulnerability out there. The one case that comes to mind was a number of years ago. It actually did not affect any funds that we were holding. But we were representing both the buyer and the seller in the transaction. And the attorneys were closing attorneys were emailing each other back and forth. Unbeknownst to us, there was a hacker that had infiltrated one of the email systems, we're still not exactly sure which one, but as Randy indicated, they were kind of waiting in the wings anonymously. And once financial information was being shared via email, the hacker came in and changed the wiring instructions at the last minute posing as one of the attorneys. So the buyer's attorney who had been scheduled to provide $185,000, to close a sale, at the last minute received an email to redirect those funds to a different account. He thought it was the seller’s attorney giving him those instructions. The money was wired, and gone, basically. So the seller’s attorney eventually said, Wait a minute, we haven't received the funds. Where are they? Well, I, we wired them to you, as you requested? Well, it was bogus. The buyers had already moved in this was this was basically the day of closing, the buyers moved in. Seller has no money for the sale of their home. And it took months and months for the authorities, attorneys, insurance companies to sort it all out. And they finally were able to partially recover and through insurance policies make the make the seller whole. But obviously, that's a huge amount of money to all the sudden have evaporate.

**Janelle**: Yeah, it's huge repercussions when, you know, businesses like what you guys are doing are affected by this. I mean, just listening to you. It's actually two different platforms, you're talking about two different email services. And still both of you were impacted. Let me ask you this, Bill, because one of the things I question is, when something like this happens, you know, when your phone system is hacked, or your email wire fraud, can you walk the listeners through sort of what you did? Like, what was the first thing you guys did you call the police? What do you call?

**Bill**: Well we pretty much called everybody we thought that might be able to help, right? I mean, you know, again, certainly when this happens to you the first time, you're not really prepared for it, even though you may think, you know, you've done the necessary things to train yourself and access resources and so forth. So just made a list of all the various different providers that might be able to help us, so we call it our IT provider. We call our errors and omissions insurance carrier as well as our business professional liability carrier. We call the local police authorities, the county sheriff, they were in touch with the FBI. And then we also called our internal corporate attorney just to get guidance on how we should be trying to navigate this. And of course, there were the other two parties and the seller, and the buyer and their two attorneys though, were all in the conversation. So it was a team effort. But we didn't know where the solution would come from. So we made sure we involve as many people as we could.

**Janelle**: Randy, what about you? Because you had similar circumstances? What did you do when this first happened to you?

**Randy**: Well, as far as the wire instance, luckily, we did. We caught it. And we found in our settings that our emails were being forwarded. We notified escrow and we basically educated an office on what to look out for. Right now, I'm under the phone system ransom, you could imagine how valuable that phone number is, you know, 13 years of doing business as a company, our office line is critical. And we basically did a similar thing to Bill where we call everyone we knew I started with the local police. I did not get much traction there. Because it was outside of state lines. I then contacted all my contacts in different departments of the police, FBI and SWAT, you name it. And I called in a lot of favors. And the result was twofold. One is that outside the jurisdiction was some of it. The second part was we're not sure if they committed a crime because we don't know what the contract said. And at the time of signing up with this company, my mistake was allowing the IT company to just hook everything up and let it go. There was no contract in place. And so based on that, they consider it a civil matter. And they did not understand what was the breach of contract because the ransom was, hey, you breached our contract, and so we're going to hold back your number and now you owe money for us to turn it back on. You know, a lot of times I think we have the habits of getting into an agreement with the one push of a button, saying that you've read the terms and policies. So one is, you know, if I could go back, I would read all the terms to the policies and procedures, but two, I would make sure we have a contract that we did not. The other people we contacted was the FCC, the Federal Communication Commission, and we still have a case out with them. And then finally, I was forced to get legal help, you know, retained an attorney. And we have the settlement and demand letter out currently. So that's where we are today. As you could imagine, this is devastating, because it's not just the phone number. It's everything it's attached to. So we've had to pivot and change all of our websites, our business cards, our email, contacts, our signage, you name it, you know, it's affiliated with everything.

**Janelle**: Let me ask both of you, because I'm curious about, you know, resources that you found to be helpful during this, Bill? What about were there any resources within NAR that have helped you on this journey?

**Bill**: Absolutely, Janelle. And my recommendation would be go to the NAR website, log in, and type in “cybersecurity” in the search bar, and you'll see information on the insurance program, and a number of different articles and guides and videos on this very topic.

**Janelle**: Randy, what about you? Any resources that have been helpful to you?

**Randy**: There's a lot out there that NAR provides. And a lot of them have been very useful. The issue that I'm experiencing is that I took the reactive approach. So if there's advice, or you know, anything that could help any other agents and brokers out there, it's to stay ahead of this, read the resources, be aware that this is an actual thing going on. And we are heavily targeted, you know, especially in the real estate industry, because, you know, you think about the dollar amounts of for example, wire fraud like Bill went through you know, it's usually very large dollar amounts, and it's devastating.

**Janelle**: Sit tight, we'll be right back with a word from our sponsor.

***Mid-Reel Ad Spot****: Explore the world and travel affordably with NAR Travel Club, NAR members gain exclusive access to savings on hotels, resorts, car rentals, activities and more. Go to* [*NARtravelclub.com*](https://nartravelclub.com/v6) *and join for free today with activation code NAR.*

**Janelle**: Let's talk about social media because that's something you hear agents talk about constantly. Everyone's trying to get on social media and, you know, increase their presence. My question for you is knowing what you both know now from your experiences? What advice do you have about social media and keeping your business secure? Randy?

**Randy**: I'd start by making sure No. 1 is that all of the media sites are up to date, all of your systems are up to date with system updates and what not. Updating your passwords is critical, because I know we get complacent. And the longer we keep one password, the easier it is to break that password. A lot of us use the same password for multiple accounts, I would say separate that to limit your liability on that. And then the second thing that I would really recommend is backing up a lot of the work you've done if there's a way to do that I know what technology there's apps and programs. So technology has come around to do that. Because, you know, it's one thing to be held ransom and it's another if someone deletes your account.

**Bill**: I agree with Randy, you know, it's real easy, as he said to become complacent with your passwords. And you know, it's kind of a hassle to have to have multiple passwords and change them but I can assure you that the amount of time we spend digging out of a cybersecurity breach is way more problematic than taking the time to manage your passwords efficiently. Although social media, Janelle, is really, you know, an animal all its own, I would still lump it into the bucket of technology platforms. And I think the same principles apply, whether it's social media websites, email systems, and that is to is to stay educated. Randy alluded earlier, making sure you're reading all the terms and conditions again, how many times do whether it's Facebook or Instagram or we click on I'll accept those terms. Without reading them, knowing what each platform security utilities are, treat social media as seriously as your email system, even though it's more of a social platform.

**Randy**: I'm glad you put it out there, Bill, because it's a lot of time taken for granted that it's social. But you know, for a lot of us, it is our entire marketing campaign, you know, beyond paid advertising, right. So we're very blessed to have that tool, and it should be treated as an asset.

**Janelle**: Bill, you mentioned something about the technology bucket, which I thought was interesting. And so I wanted to ask, you know, in terms of technologies, have you implemented, purchased, adopted any new technology since this happened?

**Bill**: Well, we've certainly had our IT folks and our vendor in to do a 360 analysis of what our protections are, and we had protections in place, but, you know, things like firewalls and various different anti-virus software we had in place, but it's sort of a cat and mouse game. You know, the hackers and the bad actors out there are constantly developing new ways to infiltrate systems. So you can't just remain static with the protections that you have in place. I'm not an IT expert. So I, you know, rely on the vendors that we use to help protect us, but it's constantly under review.

**Randy**: Each computer should have a good program that's consistently updated, because once they get outdated, the day after it's outdated, you're a big, big target. And there's a big opportunity for people looking for that little window, right? I love multi-step authentication on devices, it has saved me from potential issues that we've encountered in the past prior to that technology. Escrow has piggybacked with us and provided different wire protocols and encryptions, and encrypted emails, and that has really helped bring down the liability on that.

**Bill**: Certainly, this is a technology issue, no matter how robust your technology security is, I think the piece that we sometimes forget about is education, particularly for all the users within our organization. So oftentimes, the infiltration comes because somebody's answered an email that they shouldn't have opened up. You know, there's nothing foolproof, you know, if your staff is trained on what to look for. Back to the example I cited earlier, that $185,000, the attorney that allegedly requested the wired instructions to be changed, was in control of a hacker and they just added a digit to the end of the attorney’s email. So if it was John Doe at Gmail, the hacker use John Doe number one, and you know, wasn't enough of a difference for the user to notice.

**Randy**: To piggyback on that when we intercepted the wire instructions, we noticed that the wire instructions was one digit off, and all that simple catch led to prevention.

**Janelle**: Wow, no, that's good advice to just pay attention and really be diligent. I think that was very good to say that last question for you both because I think it's fascinating what you've experienced. I'd like to know what are the top three things you would advise your peers to do you know, knowing what you know now and what you've been through? Bill, what are the top three things you would tell them to look out for?

**Bill**: Well, number one I just mentioned that would be education. So as a broker/owner, learn for yourself the ins and outs of this cybersecurity world and NAR as you mentioned, Janelle are asked about has great resources written and provided from a realtor professionals perspective. So I would start there, but definitely education for yourself and everybody within your organization. Because again, anybody on your team is a vulnerable entry point for a bogus email. The second point would be to make sure that your insurance policies are properly set up. That would include your errors and omissions policy, which in many cases does have the opportunity for a cybersecurity element, as well as your business owner policy liability policy. There's lots of insurance options out there but I would definitely recommend connecting with a carrier an agent that knows the cybersecurity space and then I think the third item would be you know, if you don't have the capability of navigating the IT world internally, if you're not a really large company, identify an IT provider that can make sure your networks and your email systems are set up in a proper way with the most advanced technology safety nets in place.

**Janelle**: OK, those are good tips: education, insurance and IT. Randy, what are your three?

**Randy**: Thank you for sharing, Bill. Sure, the number one most critical thing, in my opinion is to stay ahead and stay educated just like you said. And to elaborate on that, No. 1, I wouldn't take things for granted, cyber fraud is on the rise. It's the real deal. And I can't tell you how many other brokers and being a being a director on our board, we've heard about multiple instances that did not have such a happy ending that you did Bill, I've heard of clients actually losing the entire wire, you know, which could be the amount of a house and they never did recapture that money is. Number two is that create policies and procedures, just like most of us already do. My company, for example, does not accept wire instructions from escrow. Nor do we accept Statements of Information from escrow it goes directly from escrow to our clientele, through whatever cyber procedure they have, or wire procedure, which kind of limits the liability on our side. And then second of all, they have the technologies to protect against those specific things more than we do. So piggybacking with good partners is great. The third thing is that utilizing the cyber fraud and wire disclosures that are provided, usually by our associations, you know, really set us free in the future, stay ahead and stay educated. No. 2, my IT company and gentleman, he's like a broken record for our office and he says, treat your passwords like you would a toothbrush and change them quarterly. I take that seriously. And then the third is cyber insurance, adding the additional cyber insurance, which is now offered by most insurance companies, there's the basic and then you can up the dollar amounts within it. But there's also an additional coverage feature, which is kind of like a rider you can add on. And you can do it through your E&O insurance, and I believe you can add it onto your business liability insurance as well. So those are three things I would highly recommend.

**Janelle**: Randy, Bill, this has been some really, really great and useful information. Thank you both for joining and sharing these nuggets with us.

**Randy**: It's my pleasure, Janelle.

**Bill**: Thank you, Janelle. I hope it helps.

**Janelle**: No, it's very helpful. And that concludes today's episode. I want to thank everyone for listening. And until next time, this is Drive with NAR.

***Outro****: Thanks for joining us on this episode of “Drive With NAR.” Tune in every month on* [*Magazine.realtor/drive*](https://magazine.realtor/drive) *or subscribe wherever you get your podcasts. Get more tips to boost your business at* [*Magazine.Realtor*](https://magazine.realtor/)*.*