**Drive With NAR: The Safety Series**

**Your Information is Probably on the Dark Web**

**Tracey Hawkins** ([00:00](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

It's an underground world online where your personal information, your brokerage's information, and your client's information are being traded and sold.

**Burton Kelso** ([00:08](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

It's where a lot of information winds up in large scale data breaches.

**Tracey Hawkins** ([00:11](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

The dark web is a clandestine dimension of the internet that many people don't understand, but all the ammunition is there for hackers and scammers to attack your business and transactions.

**Marki Lemons Ryhal** ([00:23](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I do not want anyone to join me who I did not invite to the table.

**Tracey Hawkins** ([00:29](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Now, is there anything that you can do to stop your data from reaching the darkest corners of the web? Yes, and in fact, it's entirely up to you.

**Burton Kelso** ([00:38](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

People are usually responsible for their own breaches because of negligence on their part.

**Tracey Hawkins** ([00:47](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Thank you for joining us on Drive With NAR, The Safety Series. I'm Tracey Hawkins. Let's talk about the most important cybersecurity, hygiene. Your business needs to prevent your sensitive information from ending up on the dark web and in the hands of bad actors. I am so excited to introduce our two guests, two technology experts who will help us understand this. First we have Marki Lemons Ryhal, a real estate broker, keynote speaker, and host of our sister podcast Drive With NAR: The REALTOR® to REALTOR® Series. Hi, Marki.

**Marki Lemons Ryhal** ([01:20](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Hey, how you doing today?

**Tracey Hawkins** ([01:23](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I am well. Happy you're here. Next up we have Burton Kelso. He's a keynote speaker, owner and chief technology expert at IT support company Integral. Hey Burton.

**Burton Kelso** ([01:34](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Tracey, what's up?

**Tracey Hawkins** ([01:35](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Nothing much. Thank you both so much for being here during Cybersecurity Awareness Month. Burton, we are going to start with you. Mr. Tech, can you talk to us a little bit about this mysterious dark web that we keep hearing about? Tell us why that's important in the real estate industry.

**Burton Kelso** ([01:52](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Well, the dark web plays a big role in the real estate industry because it's where a lot of information winds up in large scale data breaches. Now, I don't want everyone to think that the dark web is just this huge scary place. It's just where cyber criminals do business, but also legitimate businesses work on the dark web. When we talk about the internet, only 10% of the internet is the space that we use. So if you're on Netflix, checking your email and just using social media, that is the top web or the known web, but the dark web businesses utilize. But unfortunately, cyber criminals utilize the dark web, which is why it's important for you to be aware of what information of yours may be lurking on the dark web.

**Tracey Hawkins** ([02:37](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I just recently interviewed a Colorado Bureau of Investigations cybercrime agent, and I said, what message do you have for the real estate community? What can I tell them? And she said, tell them that you are the target. Burton, why is the real estate industry a target for the cyber scammers?

**Burton Kelso** ([02:56](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Because real estate transactions involve so much money. They may be with a brokerage, but at the same time, they may not have the protections from that brokerage as far as IT support is concerned. Many are mobile, which puts them at greater risk for cyber criminals to be able to attack them. Unfortunately, there's so much to know when it comes to real estate business and with real estate transactions. And for most, cybercrime is the last thing they think about when it comes to making sure that their data is safe and their buyer and seller data is safe as well.

**Tracey Hawkins** ([03:30](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Now you're the tech guy, you're the hands-on tech guy. I've got to ask you what tool is out there so that agents can know whether or not their information is on the dark web and how do we use that tool?

**Burton Kelso** ([03:40](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Well, there is a website called haveibeenponed.com, to go and check and see if email addresses have been leaked onto the dark web and as well as phone numbers. Because the challenge with information being onto the dark web, normally when companies are breached, they don't notify everyone that they've been breached. Now we've seen Target, we've seen T-Mobile and other companies disclose when they've been breached, but for the most part, there can be smaller businesses that kind of slip under the cracks and when they get breached, they don't report it. So it's very important for you to go to haveibeenponed.com to verify that your information isn't floating on the dark web. And if it is, then you can take steps in order to protect your information. So cyber criminals can't use it to their advantage. You could go to www have H A V E I, the letter I, been, which is B E E N, poned, which is P O N E D.com.

**Tracey Hawkins** ([04:44](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Marki, you are a social butterfly. You're also a social media expert. One thing I wanted to talk to you a little bit about is behavior online that could jeopardize not only the agent but the consumer. You talked about licensed law and the REALTOR® code of ethics and behaviors. Can you talk a little bit about those as it relates to those real estate agents who are on social media?

**Marki Lemons Ryhal** ([05:09](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Yes. The very first thing I realized, I had taken a train one year from Chicago down to Springfield for our legislative meetings. A young gentleman had gotten on the train, I could hear that he was in distress. He asked me if he could use my telephone in order to call his father. Soon as I handed him my phone, I had this feeling that, you know in your gut, and I'm like, oh, I just gave him my mobile device with every single app being open, think about your email addresses. Think about if you use Google Drive, if you are utilizing Dropbox, he had access to it. That means that they can take screenshots or send themselves files from your device. Well, come to find out he wasn't calling his father. He was actually calling his boyfriend who was ignoring him, and he wanted to call him from a different telephone number.

**Marki Lemons Ryhal** ([06:02](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

And I realized that once he had given my phone back, everyone who he had texted. So when we arrived in Springfield, he asked if he could use the phone again. And I said, absolutely not. But what I learned from that lesson was not only can I not ever allow strangers to use my mobile device, but I cannot allow my husband to use my mobile device or my children to use my mobile device because when we think about confidentiality, we owe it against even the people in which live in our house, which is also why I don't talk real estate business in front of my husband or my children or let's say confidential information because your children have recording devices. Another thing that I learned, and they record us for the purposes of becoming famous on TikTok and Snapchat, and I'm one of those parents that you can provoke, and you can get some really good cursing language out of me. And so I know what not to do. And the mobile device has access to every single business file that most of us have. We cannot allow anyone to touch those devices, and we need to make sure that we have strong passwords on those devices.

**Tracey Hawkins** ([07:13](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Okay, now Burton, I know you're going to talk about passwords versus past phrases. Tell us why pass phrases is what we need to focus on

**Burton Kelso** ([07:21](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Real quickly To back up what Marki said, don't only think about family members. Think about those smart home devices that you're sitting around doing real estate transactions. Google and Alexa are always listening to your conversations. So beware when you're talking around your smart home devices. Now, as far as passwords versus pass phrases are concerned, as humans, we get sentimental when we come up with passwords. And so we normally use passwords that are tied to things that we post on social media, memaw or mades, uh, birthdate, all sorts of things that are tied to our personal lives, which make it easy for cyber criminals to hack our passwords. If you get into practice of using pass phrases, then you are starting to move away from that personal stuff and use pass phrases that aren't related to you. Pass phrases consist of two unrelated words that create a strong pass phrase. So for example, you might want to use the pass phrase of Yellow Rhinoceros 1925 exclamation point, or maybe you want to use Maroon Camaro 2023 exclamation point, but those past phrases aren't tied to you and it's harder for criminals to figure those out. And if you struggle with making up your own past phrases, there's a website. It's use a passphrase.com where it'll generate passp hrases for you to keep those online accounts safe and secure.

**Tracey Hawkins** ([08:46](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Now let's talk a little bit more about ways to stay safe online. The 2023 Member Safety Residential report by NAR did a survey. One thing that they talk about is residential members who are likely to encounter crimes after receiving a threatening or inappropriate email, text message, phone call or voicemail. Thirty percent of the time somewhat related to that. Marki, you have a story to tell, you have a lot of great stories, but you have a story to share with us regarding your location when you were on social media.

**Marki Lemons Ryhal** ([09:18](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Well, what's kind of funny is actually NAR wrote an article about me being the barrenness of Hyde Park. I do a lot of location based check-in, and at the time there was an app called Square and I also would check in on Yelp. Now, one of the reasons for checking in is because it's gamification. And there were two gentlemen who I was kicking their tails, okay? And I would get free things like appetizers or cocktails or dessert. So one day I'll never forget, I was having lunch in Hyde Park, the community that I was the bareness of, and I was at a local sushi restaurant. And while I was there, I posted a picture of what it was that I was eating in real time. By the time my meal was over, a person was sitting across the table from me who saw my post and decided that they would join me. The lesson learned from that because most people will say, well, I'll never post again. No, take your beautiful pictures. I still do it all the time, but now I post once I have left the premises because I do not want anyone to join me who I did not invite to the table.

**Tracey Hawkins** ([10:39](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I cannot have a conversation about cybersecurity without talking about all of our second love artificial intelligence. As a matter of fact, all of my cybersecurity training now revolves around artificial intelligence. Cyber criminals are using these same tools against us, against the community. So here's what I want to do. Both of you talk about artificial intelligence, you both do training. Burton, can you summarize what you talk about when you're talking to agents about how to use artificial intelligence in their business? And then I'm going to talk about how cyber criminals use it. Burton, what are you talking about?

**Burton Kelso** ([11:16](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

The same things that you're talking about, Tracey, the fact that cyber criminals are using tools like Bard and Chat G P T and Binging Chat in order to commit cyber criminal acts. Now, fortunately, AI is caught up, so, but criminals do still have access to websites like fraud, G P T and Worm G P T, where they can create convincing phishing emails and text messages in order to trick realtors out of their valuable information and to trick their buyers and sellers to commit wire fraud. So I mean, those are the things that I mainly talk about when it comes to AI.

**Tracey Hawkins** ([11:52](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Right? And that's something that people get excited after Marki gets everyone all worked up and Marki talk to us about the training that you offer because you've taken the ball and you have run with it.

**Marki Lemons Ryhal** ([12:04](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

So when it comes to artificial intelligence, in six months, I was able to increase my productivity by 210% and my income by 283%. So needless to say, I absolutely love artificial intelligence, but in my classes I teach about deep fake voices and deep fake imagery, right? Where someone can essentially hack your voice and hack your lookalike version of yourself. We were seeing it a lot on television until they went on strike. We had just started to see deep fakes in all of the different TV shows, whether that was from Law and Order or SWAT. So we're not seeing it as much now, but it is real with very low cost. And some of these tools still, you could use the free version, how someone can sound like you and look like you. So we have to be very cautious even when it comes to those emails, they don't have as many typos. So we have to be cautious to text messages, to emails, to telephone calls. And often people will say, oh, well then I'm never going to create video. No, I can call you and clone your voicemail so they can clone any audio that they have of you. That's not a reason to not do it, to market your business. But we have to implement strategies. One that we need to know what it looks like and what it sounds like so that we can then protect ourselves, especially when we receive it.

**Tracey Hawkins** ([13:30](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

One story that I keep hearing is that broker phone call story. Everyone has a story about getting a text message or a call from the broker saying, I need you to go get a gift card. Um, I have this client, I need to gift card. Call me back and read the number. And agents were doing it. As unbelievable as it sounds, what cyber criminals are doing is they're using artificial intelligence tools in order, just like you said, to impersonate and clone their broker's voices and call to ask for this information. And they're also calling the accountant the accounts payable and saying, pay this invoice. And if training is not done in the industry, alerting them that this is happening, there are going to be a lot more stories in the headlines. And Burton, I know you can relate to this, I had an opportunity to talk to a representative from the MLS that got breached than made national headlines. And it basically shook up the industry for a while. Real estate agents were not able to access the property information, whether or not they're available, consumers couldn't access it. I asked him, I said, what do you advise the real estate community? What message can I take from you to them? He said to tell them to tighten up. So when we're talking about tighten up, Burton, talk to us about tools that can be used to tighten up, including VPNs. And you mentioned the SIM card fraud.

**Marki Lemons Ryhal** ([14:51](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Talk to us about that.

**Burton Kelso** ([14:53](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Well, first off, we all have to realize that cybercrime is a human problem. Meaning that people are usually responsible for their own breaches because of negligence on their part. That includes clicking on scam emails that may come into your inbox or text messages or even making sure that you have strong passwords or pass phrases for your online accounts. We're seeing a wave of social media accounts being attacked, and a lot of this is because people haven't changed their passwords for their social media account. People forget that LinkedIn was hacked back in 2017, and I guarantee there are people still using that old password that they had with LinkedIn, but it's floating around on the dark web. But some of the tools that agents can use in order to keep themselves safe is number one, I'd highly recommend that you would set up a Google alerts for yourself as a real estate agent.

**Burton Kelso** ([15:41](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

So that way if a criminal tries to impersonate you, then you will get an alert that there is a fake account or at least a fake appearance of you on the internet. As far as your cell phone number, you got to get out of the habit of sharing your mobile number with your buyers and sellers. The only people in this day and age that should have your mobile number are close family members and close friends. Everyone else you need to set up either a free WhatsApp to have a real estate number. You can use Google Voice. If you don't feel comfortable with free, there's always RingCentral and Vonage that agents can sign up for in order to make sure that they're keeping their mobile phone number safe. Because if a criminal gets access to your mobile number, they can call your provider. They can impersonate you with a deep fake scam or deep voice cloning scam. They can impersonate you, call your cellular provider and have the number transferred from your phone to their phone and then they can commit fraud. And of course, you're going to lose buyers and sellers. So you definitely need to protect that cell phone number like your life depended on it.

**Marki Lemons Ryhal** ([16:47](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

When I think about the M L SS hack that occurred, I was actually at a REALTOR® association that day that was subject to that hack. First of all, it is a huge distraction. So over on Drive With NAR: The REALTOR® to REALTOR® Series, we had the opportunity to do an interview. And basically what they're telling us is we need to be prepared for future occurrences. That means that everything that we're providing for them today, they need to implement. And one statistic we haven't discussed is the fact that 80% of real estate brokerages are going to be small to medium companies, which is why they are always coming after us because they know that safety is often on the back burner for us. But more importantly, what came out of our discussion is the fact that when they tell us to update our devices and update our apps, we need to do so because there's likely a breach and they're fixing that breach. And so when you receive any notification that there is a update needed, we are to update our apps and our tools to essentially close the door that was left open to allow people in.

**Burton Kelso** ([18:01](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I'll add to that too, Marki, that there is a big bounty that all of the tech companies put out. So there are hackers that are actively trying to see if there are breaches in said software and hardware. And if they find them, they get a large reward. And like you said, Marki, the update goes out and absolutely you've got to download those updates. I think people ignore that because it's the old adage of, well, if I update my device, then there's going to be a glitch or a bug. But those days are gone. Update your stuff like Marki said, because it's a matter of losing your information and losing your buyer's and seller's information. And no one wants to be that agent that has to say, Hey, I'm sorry I was breached and your information's out there, you're going to be out of business in six months or less.

**Tracey Hawkins** ([18:46](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

We often have to put this in dollar terms for agents to really feel the impact. The cost of a data breach in 2023 was $4.45 million according to IBM. Marki, both you and Burton had a conversation about verified social media accounts and Marki, you had an issue with your social media, your Instagram account. Can you tell us a little bit about what issue you had? And then I want Burton to jump in and talk a little bit about how, what protections verifying an account offers.

**Marki Lemons Ryhal** ([19:20](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

So yes, I, I had an issue for like six weeks. Someone continued to clone my account and so I'm Marki Lemons, right? They would add two Rs to the first name, then two Ks, and they had changed their, username essentially 14 times. And when I would go look their account up, oh, I had to <laugh>. I couldn't use my account to look their account up because they had blocked me. When I used my husband's account to look their account up, I realized that they had changed their account 14 times, but it was an account from a foreign country. And so becoming a clone and putting that little blue check mark what has cut down on the amount, because easily in my bio I can say I'm a verified account and this person clearly was into the crypto business. I had at least 100 people inbox me a screenshot of their conversation because it was a totally new conversation from what I was having with people.

**Tracey Hawkins** ([20:26](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Burton, you're a Mr. Hands-on IT Guy. Talk to us about verified accounts and what protections they offer and which protections they don't offer.

**Burton Kelso** ([20:35](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

If you're someone like Marki and you have a large social media following, having a verified account can be a positive thing because number one, criminals attacked Marki because she has a large following and they want to be able to fish to those people connected with her through social media. But the challenge is even though you have a verified account, you just can't rely on the verification process on itself. The positives are that yes, your account is verified, people will know that it's your account as opposed to a cyber criminals account, but you have to be aware because cyber criminals are starting to be able to get verified accounts themselves. So you still have to do your due diligence, like if you had a standard social media account and make sure that you're using strong passwords or pass phrases to protect your account. And most importantly, you need to set up two-factor or two-step authentication for all of your social media accounts. And the challenge is a lot of social media accounts are being hacked because people haven't turned on two-step authentication. But on the flip side of what happened with Marki, her account was cloned, which means that criminal or criminals have taken her information, created a fresh account. So again, you have to stay on point and make sure that your followers are protecting you as well. And if they see a cloned account, make sure that they know to report the fake account.

**Marki Lemons Ryhal** ([21:58](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

You know what I’m noticing? There's a cycle. So we were all going through the cloned Instagram accounts around the same time. What I'm noticing now are the direct messages to your Facebook business page that states something about meta. I get one to two of those every single day. So it's like it's the new popular crime.

**Tracey Hawkins** ([22:20](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Let us wrap up with something that I know is top of mind with every real estate agent out there trying to be the social media person to get business to grow their business. The appearance of being successful, and I know this is a big deal in the luxury market. One thing that I have been saying for years and finally it took the pandemic to make it happen is that agents need to work in a virtual manner. Having your first meeting virtually is not only safer, but it's more productive. You can share the screen and show would-be clients, properties before you waste time and go pay $6 a gallon for gas and show them properties that they just don't like. So it's a great way to be productive as well as to stay safe for that first meeting. You can also determine the demeanor.

**Tracey Hawkins** ([23:05](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Are they upset, are they agitated, are they motivated? So I think working virtually is ideal. One thing that I heard from an agent is that she would do virtual open houses. She would go live on Facebook, do virtual open houses, but she would not share the location. She would say, if you want the location, you need to text me, email me, or send a comment. That was smart for two reasons. One, she was verifying who they are that she could actually contact them. And second, it was great for lead gen. I want each of you to talk to the real estate agent out there who wants to be on social media, who wants to show that they are successful so that they can grow their business, tell them what they need to know about doing that successfully, but being safe doing it. Marki, what's your advice?

**Marki Lemons Ryhal** ([23:51](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

My advice is video is still the most engaging form of content and of course live video is going to put you right at the very top. However, video is still the most engaging form of content. So you can prerecord your video content and have the second most engaging form of content because you can repurpose that video content into at least 200 different forms of content. And so one, you understand whether or not you have someone accompanying you at that open house, whether it's advantageous to go live. If they've already marketed the property and done a lot of other marketing and people know they're there, then I would say they would might definitely want to have someone to accompany them. So not using the address in real time is 100% okay. Especially if it accompanies a landing page with viable information like down payment assistance to be able to buy that property.

**Marki Lemons Ryhal** ([24:44](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

If you're interested in pre-qualifying for this property to see if you can get this grant program, click on the link and we will set up appointment with you, a virtual appointment within 24 hours. We have to think creatively and outside of the box. And I do understand a lot of people want to be first. I have realized as I age, I don't ever have to be first. What I want to do is be the best. And in being the best, that does not require being number one. It often requires sitting back analyzing what number one has accomplished and then doing it in a new way.

**Tracey Hawkins** ([25:20](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

And I like that you said you can be live because of the algorithm, but you don't have to share the address. So agents, there are ways that you can do your job safely and still be productive. Burton, talk to us a little bit about that. What is your advice? Are there any tools or anything that agents need to know regarding working virtually and safely at the same time?

**Burton Kelso** ([25:42](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

Yes, absolutely. So probably your best friend, if you're working remotely and you want to keep your information safe and secure would be to enable a VPN on both your smartphone and on whatever mobile device or even your home computer. Because a VPN is going to mask your location, you can say you're anywhere in the USA and that information won't be leaked to criminals. Another thing you have to be careful of is metadata attached to photos. If you are taking photos, at a property, you sometimes have to be careful of that because the metadata will expose the address or the general location of the property. However, if you're taking photos showing how luxurious you are as a real estate agent, you don't want to take those around your home because that same metadata can pinpoint where you are and then it can allow cyber criminals to reach your location. So in that aspect, always be careful of the metadata that your photos and videos are sharing and make sure that when you are doing listings and if you're doing videos for a virtual showing that you are using a VPN to keep your location safe and secure. And one thing that we forgot to talk about for cyber data is backing up all of that information, backup, backup, backup, and make sure that it's an automatic backup system that you're using to keep all of your real estate information safe and secure.

**Tracey Hawkins** ([27:10](https://www.temi.com/editor/t/-VzW9jtvWyFpKXdy-Kcvh5Ntr9p9XLHOUNXMxlBihqoeO2d3bEbPNeO277vB6lXa_IJ65Ji-p_mw3unzd4dy89wLzm4?loadFrom=DocumentDeeplink)):

I want to thank you all so much for joining us today during Cybersecurity Awareness Month. The tools are there, the information's there, you just have to implement it. Thank you all so much and be 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 podcasts. 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.