Cyber Security and the Law (Lake Oswego)

Real estate professionals are invited to Cyber Security and the Law: How Do You Protect Yourself and Your Clients as a Real Estate Professional? Ken Perry of The Knowledge Coop will guide attendees through questions and statistics to help you and your clients.

Registration is $12 per person, and 2 CE is available for Oregon attendees. Attendees must register even if CE credit is not desired. Read more or register online for Cyber Security and the Law.

REALTOR® Safety Month: Electronic Safety

The FBI operates a website dedicated specifically to internet crime. Image: FBI.gov

September is REALTOR® Safety Month! This is the second of two articles covering safety issues of particular interest to RMLS™ subscribers.

Remember the days when frauds and scams were easier to recognize and seemed like the type of things "other people" had to worry about? Technological advances have brought plenty of new tools, devices, and apps to improve organization and efficiency. Unfortunately the sophistication and prevalence of

frauds and scams has advanced just as quickly.

AWARENESS

At any time, there are a number of common frauds and scams circulating both locally and globally. It used to be simpler to detect email scams, whether by blatantly odd email addresses or oddly conjugated messages—but former red flags are getting more difficult to detect, as scammers' methods are continuously gaining sophistication. Here are a few red flags to look for.

Emails regarding wire transfers or containing wire transfer information: RED FLAG

Double and triple check your contact's email address. Hackers will often observe email correspondence discussing wire transfers, then intercept the communication, posing as your contact. They imitate the language used in previous correspondence and include wire transfer information funneling into a fraudulent account. Often, the account is emptied and closed as soon as the wire transfer has occurred.

What to look for

Check the email address and carefully confirm its validity. For example, if you are expecting an email from angel.rmls@123.com, notice possible imposter email addresses:
ange1.rmls@123.com
angel.rm1s@123.com
angel.rmls@l23.com
angel.rmls.@123.com

Each of the above addresses vary from the first with a single, minor change. The replacement may replace the letter "L" with the number 1 or add an inconspicuous dot—but at first glance they all look very similar to the original address.

Emails requesting last-minute changes to wire transfers or monetary exchanges: RED FLAG

What to do

Check and double check your contact's email address. Call your contact on the phone to confirm that details and changes are legitimate. Be alert and trust your instincts if something feels off.

The National Association of REALTORS® (NAR) has a great article addressing sophisticated email scams and damage control.

Attachments or suspicious links: RED FLAG

There are a significant measure of viruses spread via email attachments and links. When opened, the virus wreaks havoc on devices and confidential information. In some cases, the attachments can be sent from a familiar email address that has been hacked.

What to do

Stay alert and look out for oddities. Were you expecting the attachment or link? Confirm with your contact that they sent an attachment or link intentionally—sometimes this is how people discover they've been hacked in the first place.

DocuSign recently experienced fraudulent activity which the Oregon Association of REALTORS® addresses here.

Another challenge to the local market is the Craigslist scam where photos of listed homes on the market are scraped and posted on Craigslist as being up for rent. Craigslist has quite a bit of information detailing what to do in these situations.

PREPAREDNESS

Your electronic safety can be greatly enhanced by an established data security plan, including best electronic practices, damage control, and reporting tools. Below are a few best practices for cyber safety:

- If sending an email with monetary transaction information, utilize encryption services whenever possible.
- Be wary of messages from unverified accounts and avoid including sensitive information to these accounts.
- Do not reply to suspicious accounts and never open attachments or links from suspicious accounts.
- Utilize strong passwords and change them regularly.
- Utilize secure networks when conducting business online.
- Stay up-to-date on software, anti-virus, and browsers.
- Think defensively at all times and be alert to cyber threats.

NAR offers a useful article discussing best practices and policies for cyber safety. Does your office have an established data security plan or document retention plan?

DAMAGE CONTROL

If you have a data breach, there are a number of actions that may help with damage control:

- When wiring money transfers, confirm receipt *immediately*.
- If you've been hacked or click on a link that locks your screen, shut your machine down *immediately*.
- Inform colleagues if they may have been exposed as a result of a data breach. Provide as many details as you can, and inform your IT department or manager.
- Change all of your passwords to ensure they are strong.
- Report the breach to the FBI Internet Crime Complaint Center.

- Report the breach to your local REALTOR® association.
- Report the breach to RMLS™ by contacting Michelle Gray at (503) 872-8059.

Cyber safety is incredibly important for everyone. RMLS™ urges REALTORS® to stay informed and be alert to remain safe!

Tips and Resources for REALTOR® Safety Month

Safety should never be relegated to just one month, but September is REALTOR® Safety Month. This year marks the 10th year of the National Association of REALTORS® (NAR) dedicating a month to REALTOR® safety. Every year more and more alarming (and sometimes bizarre!) stories emerge from our subscribers: robberies, creeps, and fools. Every year RMLS™ strives to give subscribers resource material to better educate and protect themselves.

Top Tips from NAR (and Me)

The following are the four most paramount tips NAR would like to pass on:

1. **Have office guests sign in.** At the office, use a visitor log book where potential clients fill out a customer identification form. Remember to check IDs.
2. **Don’t disclose too much personal information online.** Consider setting up separate personal and business accounts on Facebook, Twitter, and other social media sites. This will help protect your personal photos, posts, and other information from people you don’t know.

3. **Familiarize yourself with the properties you're showing.** If you are showing a vacant house, walk the perimeter of the property before you or your client enter to look for signs that someone has been or is currently inside.
4. **Note your escape route.** When showing a property, leave the front door unlocked for a quick exit if needed. As you walk through a house, let the client enter rooms ahead of you.

And my personal favorite tips:

1. **Tell people where you are going if meeting someone alone or for the first time.** You can also go so far as to have a colleague call you at a certain time if you are nervous about the meeting. Mention the name of who you're meeting and even set an estimated time of return.
2. **Reasonable people will answer reasonable questions.** For instance, there has been a rash of would-be buyers who are offended when asked to provide proof of funds for an all-cash transaction or who become upset if you can't meet with them under their conditions. While it's not always the case, dramatic reactions to seemingly benign questions or comments should raise concern.
3. **Advise your sellers of the possibilities.** Tell them to lock up all valuables, especially small items such as prescription bottles, checks, and jewelry. Even at a brokers' tour with the most seasoned agent, someone who doesn't look suspicious who says they were in the neighborhood and saw the sign can wreak havoc and you know the rest.

Technology. Whew, What They Can Do These Days!

In our last safety post, we discussed internet resources REALTORS® could utilize to be notified should their listings be hijacked by scam artists and posted on sites like Craigslist and even Trulia. Now you can empower yourself with applications on your mobile devices. Smartphones have become

ubiquitous in the real estate industry. Safety applications go beyond just panic button capabilities these days. Some applications utilize GPS coordinates for emergency response while others offer speed dialing or automated emergency messages that go to designated numbers. As new apps become available every day, check your mobile device's app store for the latest offers and information.

That said, still protect your personal information in case your phone is stolen or compromised. Consider installing a tracking device on your phone where you can remotely access it from a computer. Device passwords should be unique and free from obvious patterns like 4-3-2-1 or 1-3-7-9 (the four corners of a key pad). Read on at REALTOR.org for a comprehensive list of safety precautions for your valuables and yourself beyond those mentioned here.

Speaking of helpful resources, NAR has an archive of safety webinars for REALTORS® that include all they released in the last four years. Webinar topics on the archive include open house safety, online safety, office layouts, and removing dangers specific to distressed properties. This kind of information can be great to touch on either briefly at an office meeting, or NAR has a variety of full presentations available for your staff.

Trust your instincts, be aware of your surroundings, and always listen to the little voice, no matter how cliched or cynical, that says if something looks too good to be true…

Happy REALTOR® Safety Month, and if you would like to report an incident or concern regarding safety or fraud to RMLS™, please contact me at kelly.m@rmls.com.