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!