Sunday Column
By Grant Lopez, 2019 Chairman
8/18/19

How to Avoid Real Estate Cyber Scams

Phishing, hacking, wire fraud – these are all ways people attempt to steal from others online. As real estate searches and transactions move more and more online, the chances of being caught up in a cyber scam have become even greater.

By now most people have heard of the Nigerian prince scams or phishing emails asking for social security or banking information, but many people don't know that they need to watch out for possible scams when buying or selling their home. Cybercrimes have become increasingly sophisticated over the years and the people perpetrating them focus on situations where a lot of money is changing hands, making real estate transactions an ideal target.

The National Association of REALTORS® recently warned its members and consumers about one example, a wiring scam during the closing stage of the home buying and selling process. Hackers will break into the email accounts of consumers and real estate professionals to get details about a real estate transaction. The hacker will then send an email pretending to be the buyer, seller, real estate agent or someone else involved in the closing process and say there has been a last minute change and provide new wiring instructions; the instructions send the closing costs funds directly into the hacker's bank account.

While it may seem like there are hundreds of ways for a criminal to take advantage of a consumer online, there are just as many ways consumers can protect themselves. Here are a few tips to help home buyers and sellers recognize and avoid real estate scams:

Do not send sensitive information via email. Do not send banking information, your social security number or anything else that could be used to comprise your identity over email. If you absolutely must send personal or sensitive information via email, only use encrypted email.

Do not click on unverified email. If you do not recognize the name or email address of the sender, do not open the email. And beware of any attachments or downloadable files from unknown email addresses; they can contain viruses or provide a way for a hacker to access your computer.

Do not use unsecured Wi-Fi. It may seem harmless to check banking information using the free Wi-Fi at your local coffee shop, but using an open connection can leave you vulnerable to hackers and scammers. Only access sensitive information on your home computer or on a secured network.

If you suspect fraud, tell someone. If you suspect that fraud has or is in the process of occurring, contact all parties contacted to the transaction immediately. Unfortunately, often there is nothing that can be done to retrieve money stolen in the scam, however, you should still report the incident to the FBI's Internet Crime Complaint Center or the Federal Trade Commission.

For more information on how to safely and securely buy or sell a home, visit SABOR.com and use a San Antonio area REALTOR®.

###