REAL ESTATE CYBER RISKS

Real Estate transactions involve a considerable amount of non-public information, NPI, and money. Both are targets of cyber criminals and must be protected.

The categories of protected non-public information, NPI, vary by state, but typically include any information that could be used by cyber criminals to cause harm such as email addresses, physical addresses, social security numbers, bank account numbers, and earnings or other financial information.

The real estate agent may gather the information by having the client complete forms or ask for it in person or by phone. No matter how it is collected, it must be protected. If entered into an online system proper cyber security precautions must be taken to secure it. If on paper it needs to be locked up and not left on a desk or printer.

Email is often used to communicate between the agent and the client. Due to the sensitive nature of the information, we recommend the use of encrypted email services. If sending information when outside the office, Virtual Private Networks, VPN, are recommended to better secure communications.

Free email accounts like Gmail, Yahoo, etc. are not secure. If these accounts must be used, two-factor authentication is better than single-factor, but these accounts should not be used for sensitive information. Select a secure, encrypted email service and use it.

Under no circumstances should public wifi, such as that available in coffee shops, cafes, libraries, or other public places, ever be used. Having a password does not make them secure. The password is available to everyone and is rarely changed. These services are risky even for personal email communications. It is very easy for someone to steal your password or put malware on your phone or computer to steal information, even later on secure networks.

Wire transfers are the accepted means of moving money, especially larger sums for real estate transactions. However, cyber criminals know this and have scams designed for it.

An example. Before the scheduled closing date for the home sale, the buyer gets an email that appears to come from the real estate agent, title search firm or attorney, or another trusted member of the team. The email has the details about the closing the buyer wants; date, time and location. Also contained in the email are the instructions for wiring the down payment money. All seems reasonable. Except the account information goes to the cyber criminal's account, not the escrow account of the realtor. As soon as the wire transfer is initiated, the money is transferred, and it is gone forever. Cyber criminals do not have a refund policy.

This is not a rare occurrence. The Internet Crime Complaint Center, a division of the FBI, said that between 2015 and 2017 the number of reported victims of this scam grew 1100 percent with losses of over $56 million. And the numbers continue to grow.

We recommend confirming wire instructions emailed to you by calling your real estate agent or title attorney. But do not use the contact information in the email. The best plan is at the beginning of the relationship request a list of all the people and firms that will be involved in the closing with their accurate contact information. The realtor should provide this.

REAL ESTATE CYBER RISKS

If there are any changes have your real estate agent call you on the phone. They should not be communicated then incase the call is a scam. Call the agent using a number that you have used in the past, never one communicated to you on the call or the number that just called you.

Ransomware is another significant threat that is growing by leaps and bounds. It has become a favorite tool of cyber criminals because it is monetized immediately. Ransomware typically gets its entry into a company by someone clicking a bad link. It can also gain entry through mobile devices and Internet of Things, IoT, devices, such as smart thermostats, smart lights, smart locks. And these devices are proliferating. While all have the term “smart” in their name, they often are not smart at all and provide an insecure entry point for cyber criminals.

What does ransomware do? It encrypts all the information on your computers and servers. The cyber thieves provide the key to unlock the information upon receipt of the ransom. Payment is by Bitcoin or another untraceable cyber currency. Now, in order to make sure you pay, your information is first stolen by the thieves before it is encrypted. If you choose not to pay, they release it to the public. And there goes your reputation.

Social media is a popular way of sharing information with friends and family. And the purchase of real estate is often an event to celebrate. But never share any information on social media about the purchase, or even that you are looking. Social media is not secure. The information is sold by the social media company to many firms. Even with settings limiting who can see your posts, they are not secure and can be viewed by many people who want to steal your money. The same is true for “check-in” sites, they are ways that criminals find victims.

As a reminder, never click on links or call any phone numbers in an unsecured email.

Realtors need to be aware of the techniques cyber criminals use to steal information such as phishing and vishing, fake websites and others and how to avoid them.

They in turn need to advise their clients on what to do, not do, and the types of things to avoid.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.