MADISON INSURANCE GROUP
Business • Life & Health • *Private Client*

Protect From Cyber Criminals

MadisonInsurance.com • 888-539-3737

Cyber Security Considerations During Real-Estate Transactions

Buying or selling real estate, especially your personal home, presents a unique set of fraud and cyber-security risks. Protect yourself by understanding these risks and exercising the precautions below dur-ing real-estate and other high-value transactions.

Understanding the Risks

Several factors make real-estate transactions especially tempting to cyber-criminals.

Public information on the sale. When a home is listed online, those listing details become publicly available. Cyber-criminals can monitor listing sites to learn when a transaction is likely to occur. They can also identify the listing agent, which can lead to the identity of other key parties who will be in-volved in the transaction, such as legal and escrow teams. They can then impersonate these individu-als in an attempt to trick you into sending them money.

Multiple unknown parties. When you buy a home, you will likely engage with the seller's legal and/or escrow firms. However, you may not be familiar with these firms or the individuals who work for them. Common cyber security precautions such as conducting a "call back" to confirm the details of a wire transfer could be difficult to verify since all relationships are new.

High monetary value. Cyber-criminals target high-value deals because, if they are successful, they earn a greater return on their time and effort. Real-estate transactions are often the most expensive pur-chases a person makes, so they become a top priority for these criminals.

How to Protect Yourself

The recommendations below can help you guard your assets against fraud or theft during any high-value transaction.

Technical precautions. If you receive an email regarding the transaction, especially if that email in-structs you to transfer funds, be on the lookout for red flags that the sender is not who they say they are. Check their email address (not just their display name): is every character correct? For example, is the email from joe@citi.com or joe@citj.com? Also check the signature line, images and language in the email for anything that seems out of place. Enable multifactor authentication (also known as two-step authentication) for all email accounts used by you and your key staff and advisors associated with the transaction.

Process considerations. Before any funds change hands, always pick up the phone to double-check the information associated with the transaction. Be relentless in asking for verification of all account details. Always call to get verbal confirmation regarding any changes to the deal. When you receive a request for payment, do not call the number provided within the request itself; instead, call the main office of the company you know you are dealing with. Speak with two separate people associated with the deal with whom you have spoken before.