

Understanding Cybercrime



Cybercrime has become a major challenge for homebuyers and sellers in recent years. According to [the FBI](#), the real estate industry lost \$350 million to cybercrime in 2021 alone — a 64% rise from the previous year. However, homebuyers can guard against these threats by learning to spot the telltale signs of cybercrime. With the right tools, you can protect yourself (and your investments) from these threats.

6 WARNING SIGNS OF REAL ESTATE CYBERCRIME

Cybercriminals can be surprisingly sophisticated, often disguising dangerous scams as legitimate real estate investment opportunities. However, many schemes come with red flags that you shouldn't ignore. At the very least, they should be enough to make you proceed carefully.

1. THE PRICE IS TOO LOW

If it sounds too good to be true, it might be. Scammers often use artificially low prices to garner your interest, only to never deliver on a property. Of course, it's OK to investigate bargain properties, but if you can't quickly identify a good reason for the discount, you should move on.

2. THEY ASK YOU TO WIRE MONEY TO A QUESTIONABLE ACCOUNT

Wire fraud scams represent one of the biggest threats to property buyers. This is when a scam artist requests that you send them a down payment or wire money to a questionable account. As you might guess, the money is likely going to a fraudulent account that appears to be legit, leaving you with few options for recovery.

3. THEY REQUEST A DOWN PAYMENT BEFORE YOU VIEW THE PROPERTY

Beware of anyone who rushes you to sign a contract or submit a down payment before seeing a property. In an age in which real estate investors rely increasingly on virtual tours and internet postings to screen properties, it's become far too easy for scammers to post false or misleading images online to trick investors out of their money. Don't let a seller pressure you to commit until you've personally seen the property.

4. THEY WON'T PROVIDE A TITLE OR PROOF OF OWNERSHIP

Always request to see a title or proof of ownership for the property in question. That way, you can verify the seller's identity and that they have the legal right to sell the property. If they drag their feet or refuse to share this information, it's a major sign of a real estate scam.



5. THEY PRESSURE YOU TO CLOSE THE DEAL

It's not uncommon for sellers to turn up the pressure as a sales tactic, but be cautious about those who aggressively insist that you make a purchase. For example, a seller who mentions "strong competition" may be legitimate, but a seller who repeatedly contacts you to close the sale may be trying to scam you.

6. THEY REQUEST UNUSUAL PAYMENT METHODS

Legitimate sellers typically expect to be paid in U.S. Dollars via wire transfers. However, if a seller asks that you pay with unusual methods — such as gift cards or cryptocurrency — that's almost always a sign of a real estate scam.

HOW PATTEN TITLE PROTECTS AGAINST CYBERCRIME

The right tools can make all the difference in protecting against cybercrime. That's why Patten Title Company has partnered with [Qualia](#) to provide a tool to manage real estate transactions, centralizing the most important steps under a single, secure platform.

With Qualia, users can store their most important documents, schedule appointments, and digitally sign closing documents using a convenient, streamlined tool. And best of all, Qualia boasts industry-leading data security and privacy, essentially eliminating the threat of real estate scams.

Patten has also partnered with [CertifID](#), ensuring that cybercriminals can't access your personal information while you wire money during a real estate transaction. [CertifID reports](#) show Patten Title helped protect more than \$1.5 trillion against wire fraud in 2022.

Patten Title escrow agents also use [ZOCCAM](#), an app that guarantees security during earnest money transfers. ZOCCAM protects confidential user data from bad actors and potential fraud.

3 THINGS TO DO IF YOU SUSPECT REAL ESTATE CYBERCRIME

Let's say you've spotted some of these red flags during a property purchase. What do you do then? Here are a few steps to keep you and your investments safe.

1. PUMP THE BRAKES

First of all, slow down! It's better to lose a good deal than to have your money or identity stolen by a cybercriminal. Always perform your due diligence, making sure that a deal is legitimate. And, of course, don't let sellers dial up the pressure to get you to make a decision. Verify all the details, and take your time.

2. DON'T SEND MONEY

Never send money without being confident of where it's going. Cybercrime thrives on wire fraud scams and fake accounts, so be wary when sellers attempt to get you to commit to something that doesn't feel right.

3. KEEP ALL YOUR DOCUMENTATION

If you've spotted a potential cybercrime, you may need to contact the police or an attorney. If it comes to this, provide as much documentation as possible. This can increase the chances of catching the perpetrator and recovering lost assets.