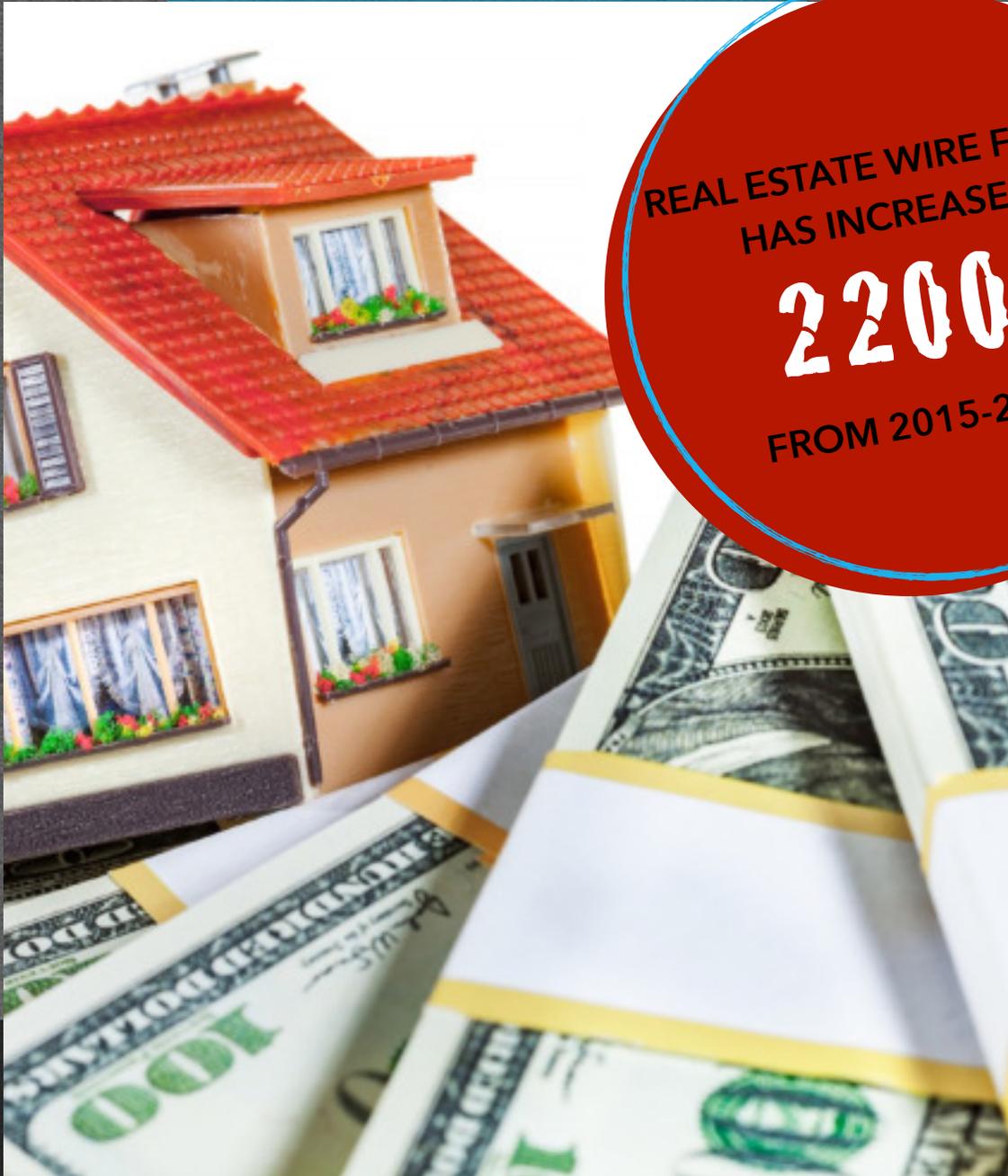


REAL ESTATE WIRE FRAUD

SURVIVAL GUIDE



REAL ESTATE WIRE FRAUD
HAS INCREASED

2200%

FROM 2015-2017

Following the five steps outlined in this guide, you will be much more prepared when a scammer tries to steal your information. If you're looking to work with an escrow company that puts your best interest first, contact OAKWOOD ESCROW today.

OAKWOOD ESCROW

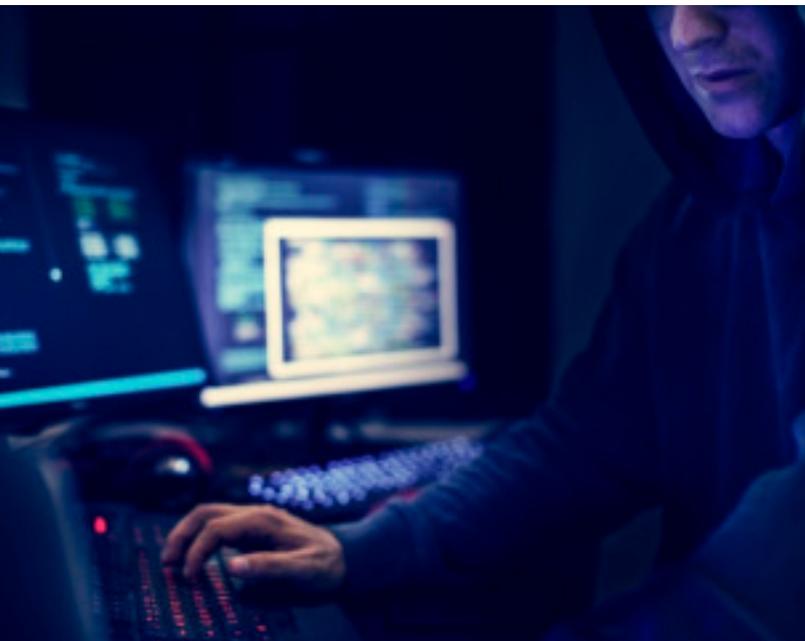
www.oakwoodescrow.com

(619) 430-4584

EAC/BAC Wire Fraud Scams are a huge problem.

While scammers are clever at mimicking professional communication to defraud you of your money, being armed with the knowledge of what to look out for can help you hone a bit of a "Spidey-Sense" when it comes to distinguishing what is a scam and what is legitimate when it comes to your crucial real estate transactions.

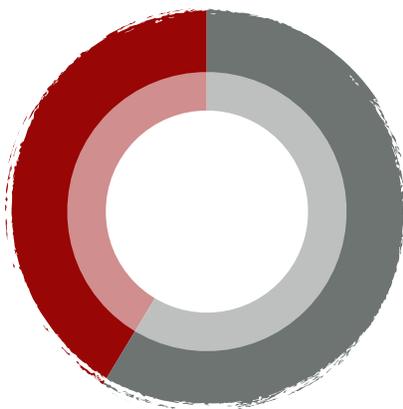
\$150 million in personal assets were stolen in such scams in 2018 alone.



Most homebuyers don't even consider the possibility of wire fraud in real estate transactions, and have false sense of security believing their banks will protect them.

Because the closing process can be so stressful, with high-pressure and fast pace. Scammers can find the information for people who are buying houses relatively easily. Using the Multiple Listing Service, along with other real estate listing websites, scammers can find houses that are preparing to close, obtain the names of all parties, and hack into one of their email accounts. Once a scammer has access to one person's email, they will use specific transaction details to lure buyers into wiring over their life savings with little to no recourse.

Catching these criminals is nearly impossible, and the lost money is rarely if ever recovered. Your safest bet is to protect yourself from falling for these scams in the first place by following these 5 steps.



- **52%** of homebuyers are completely unaware of wire fraud in real estate
- **74%** of homebuyers falsely believe their bank could recover funds wired to the wrong account

1. CONFIRM OVER THE PHONE OR IN PERSON.

EMAIL is an **extremely risky** way to do business when it comes to real estate transactions and communication.

ALWAYS confirm information over the phone or in person, especially when it comes time to send or move money.

**Always use the phone number that was given to you at the beginning of the closing process.*

If someone emails you a phone number you don't recognize, don't use it. And if you can confirm the information in person, that is even better.

The best time to confirm information is right before you are going to take any action, such as wiring money.

CONFIRM any account numbers or bank information, addresses, phone numbers, etc. that might affect your transaction and who your money goes to.



While some escrow companies still do, Oakwood Escrow will never send wiring information via email or text message.

2. KNOW HOW TO SPOT A HACKER.

If you receive an email with any information regarding your real estate transaction, you need to be **extremely aware**.

Carefully double check all of the small details, including the email address, cc email addresses, physical addresses, names, phone numbers, account numbers, etc.

If any of these are different in any way – *even if it's only by one character* – call or visit your escrow company, real estate agent, or other trusted individual to make sure the information is correct before taking any action.

Likewise, if you are contacted by phone, **do not give out sensitive information**. If someone contacts you from a phone number you don't recognize to confirm your personal information, you should hang up and dial the number you were given at the beginning of the closing process to confirm that it is a legitimate phone call.



TIP: BE WARY OF ANYONE TRYING TO GET YOU TO ACT WITHOUT DUE DILIGENCE

The closing process when buying a home can be very fast-paced and hectic, but if someone is pressuring you to send money fast, you should confirm all information with your closing agent as quickly as possible to ensure it is a legitimate request for money.

Any respectable agent should be understanding and support your efforts to protect yourself and your money.

3. USE STRONG PASSWORDS.

According to a study done in 2017 by LastPass, **59% of people always (or almost always) use the same password** or a variation of it for all of their online accounts.

Once they get one password, it's not long before they have everything.

Passwords that are too short or contain simple words, such as "password" (which is more common than you think), are easy to crack, for both humans and software.

The trouble with making long complex passwords is that they can be difficult to remember. This can be overcome by using phrases, codes, or acronyms that are misspelled or highly personal.

For example, you could use something like LivLuvLaf319<3. By mixing up capital and lowercase and using numbers and symbols, you make it harder to guess the full password.



*If you find yourself in a position where your password has been stolen, reset both that password and your email password. **Reevaluate** your other passwords as well.*

5. AND FINALLY, **JUST BE SUSPICIOUS.**

Unfortunately, there are plenty of people willing to take advantage of home buyers during the closing process. According to REALTOR Magazine, in the second quarter of 2018, the real estate industry saw the **second most malware events of any other industry.**

This means that people who are buying homes are highly targeted and should be aware of every detail through the process of purchasing their home.

Being suspicious throughout the process will help keep your eyes open to any potential threats. You should always be wary if details, such as account numbers, phone numbers, names, addresses, etc., change suddenly or if someone is trying to rush you into action. If a request is legitimate, the person requesting action or money should have no problem explaining why details have changed or why you need to act quickly.



TIP: IF YOU'VE BEEN AFFECTED BY REAL ESTATE WIRE FRAUD

- **Act as quickly as possible.**
- Contact both your bank or wire transfer company along with the bank you sent the money to and attempt to stop or reverse the transaction.
- File a complaint with the FBI. Do not rely on your bank to do this for you.
- The FBI can help by being in contact with the banks and/or the fraudulent account holder to convince all parties to cooperate in attempting to get you your money back.