NINJIO

How To Fight Back Against Real Estate Cyberfraud

For most people, the process of buying or selling a home involves the largest transfer of money they'll make in their lifetimes. From down payments to closing costs to mortgage payoffs, billions of dollars change hands in real estate transactions every year. This is why it's no surprise that cybercriminals regard the vast real estate market as one huge opportunity to defraud people and steal their money.

However, the sheer amount of real estate cybercrime (such as title and deed fraud, in which hackers impersonate a title company or realtor and misdirect transfers of funds) taking place today is a surprise. We've seen an unprecedented explosion in cyberscams targeting home buyers, sellers, and the companies they work with to complete real estate transactions. These scams are costing people hundreds of millions of dollars each year.

As with the overwhelming majority of cyberattacks, the most effective defense against real estate fraud is awareness. It's vital to know who you're communicating with, what warning signs to look for, and how to confirm the legitimacy of documents and requests – especially if they involve large transfers of money. While real estate cyberfraud is becoming more widespread and financially destructive all the time, there are many ways to fight back.

A RAPIDLY **GROWING PROBLEM**

*The most effective defense against real estate fraud is **awareness.***

According to the FBI's annual IC3 Internet Crime Report, cyberattacks targeting the real estate/rental industry cost Americans more than $56 million in 2017 – a number that rose to more than $149 million in 2018 and $221 million in 2019. Last year alone, the FBI identified almost 11,700 victims of real estate/rental fraud.

> According to the FBI's Annual IC3 Internet Crime Report, cyberattacks cost Americans **$221 million** in 2019.

Kate Rosenthal is the vice president of Chapman & Rosenthal Title, Inc., and she points out that she's working in a "targeted industry right now. Fraud is a very real problem for us, and we're dealing with it every single day." Rosenthal says she has witnessed a dramatic increase in attempted fraud over the past several years, and her company now has to spend tens of thousands of dollars on insurance that covers potential losses from fraud. She explains why it's not a shock that her industry is such a big target for cybercriminals: "They know we move a lot of money, and more and more of them are catching on."

There are many different types of real estate cyberfraud, but as with the vast majority of cyberattacks, the most effective way to protect yourself is with education and awareness. This begins with understanding the most common types of attacks and what warning signs homebuyers should be looking out for.

HOW REAL ESTATE **CYBERSCAMS WORK**

*It isn't just **wire fraud** that homebuyers have to be on their guard against – **title** and **deed fraud** is also a rapidly emerging cyberthreat in the real estate industry.*

One of the most common real estate scams is business email compromise (the costliest type of cyberattack, according to the FBI). A hacker will break into the email account of a title company or realtor and instruct a homebuyer to send funds (ostensibly to close a deal) to a fraudulent account. Once the victim realizes that the money wasn't sent to a legitimate account, the hackers have transferred it to a new account, closed the first one, and disappeared.

Companies don't have to be infiltrated for this type of scam to work – hackers will also steal personal information from other sources (large-scale data breaches at companies like Equifax can put this information up for grabs) and use it to manipulate their targets. And homebuyers aren't the only ones who are fooled – title companies, escrow companies, and other entities that handle funds have also made the mistake of transferring money into fraudulent accounts.

It isn't just wire fraud that homebuyers have to be on their guard against – title and deed fraud is also a rapidly emerging cyberthreat in the real estate industry. This type of attack relies on identity theft – cybercriminals steal your personal information so they can change the name on a title or deed and use the equity you've spent a lifetime building to secure fraudulent loans. In some cases, the thieves even sell homes that don't belong to them. Title and deed fraud can lead to foreclosure, damaged credit ratings, and other crippling financial blows to homeowners.

> *The problem in our world is that you're moving so quickly all the time. And you're having to verify and reverify information over and over.*

Homeowners who have vacation homes, rental properties, or secondary real estate of any kind are especially at risk of title and deed fraud. Not only is it harder to keep track of documentation for multiple properties, but these homeowners are also liable to ignore foreclosure notices and other alerts that could reveal fraudulent activity. This gives criminals more time to take out illegitimate loans and disappear before raising any red flags. The same applies to homeowners who have inherited properties – they often have no intention of selling, renting, or living in the home for a protracted period of time, which puts them at increased risk of undetected fraud.

Rosenthal explains that the nature of her business provides ample opportunities for criminals to steal information and infiltrate private communications: "The problem in our world is that you're moving so quickly all the time. And you're having to verify and reverify information over and over." But she says the "main thing to watch out for is email being hacked and secondary wire instructions being sent." This is why Rosenthal's company observes a concrete set of policies to mitigate the risk of fraud, such as independently verifying the legitimacy of financial institutions or any other entities involved in wire transfers.

Because real estate transactions involve so much personal information shared with many different parties (realtors, lawyers, title companies, financial institutions, and so on), they can make homebuyers particularly vulnerable to identity theft. As noted above, this can lead to title and deed fraud, as well as a wide range of other negative consequences (such as compromised accounts). Cybercriminals are drawn to real estate transactions because there's often a large amount of money involved, along with many attack vectors to exploit. As more and more hackers take advantage of these realities, homebuyers and those who facilitate real estate transactions need to be on their guard.

HOW HOMEBUYERS CAN **PROTECT THEMSELVES**

Like any other social engineering attack, real estate cyberscams work against victims who aren't trained to notice when something is wrong and take steps to defend themselves. So here are some of the most effective ways homebuyers can do exactly that.

1.

If a title company, lender, or anyone else tells you the details of a wire transfer have changed, alarm bells should be ringing. Make sure you confirm all transfers with a phone call or in person, and follow up with the recipient to make sure the funds were distributed properly. And never rely on phone numbers that can be found on documents received via email – verify numbers and any other contact information independently by checking legitimate websites and publications.

2.

Check for discrepancies in any documents and emails you receive – different formatting, contact information, names, and so on should all be cause for alarm. Rosenthal observes that the "best-case scenario is original disbursement instructions that come directly from the seller and are signed by the seller in person." Another reliable way to confirm account information is with a legitimate voided check, but this should be confirmed with the account holder as well.

3.

Make sure you find realtors, lenders, lawyers, and other professionals you trust, and ask about the cybersecurity safeguards they have in place. Don't be afraid to ask tough questions if you're nervous about something – it's your money and personal information, and you have every right to know how it's being handled. Rosenthal can point to a specific list of measures her company takes to ensure that transactions are secure and clients are protected. Every company should be able to do the same.

4.

Change passwords, implement multi-factor authentication on your accounts and devices, always use a VPN when connecting to wireless networks, even those you trust, and be extra careful before a real estate transaction. Cybercriminals are becoming more sophisticated every day, so homebuyers need to be more suspicious than ever.

Purchasing or selling a home can be a momentous occasion in a person's life – in both cases, it's often the culmination of a lifetime of hard work and saving. Cybercriminals have no respect for that hard work or the lives they destroy, and you should always remember that your most powerful weapon against them is your own awareness.

ABOUT NINJIO

NINJIO is a cybersecurity awareness training company founded in 2015 that empowers individuals and organizations to become defenders against cyberthreats. The company's Hollywood-style content teaches organizations, employees, and families how not to get hacked. Today, NINJIO serves some of the largest companies in the world, and its methodology is responsible for changing the behavior of hundreds of thousands of people through engaging, emotionally-driven storytelling.