nj.com

Real estate scams are skyrocketing. Here's how to protect your home sale.

Updated: Jul. 16, 2024, 12:07 a.m.|Published: Jul. 15, 2024, 9:30 a.m.

11–13 minutes

It's a shocking, intrusive crime. And it's becoming more and more common.

An unsuspecting homebuyer gets an email with instructions on where to wire funds for the real estate purchase. It seems to come from a real estate agent, an attorney or another person involved in the deal.

But it's a fraud.

The FBI's 2023 Internet Crime Report said New Jersey ranks second in the nation for having the most incidents of "business email compromise" scams, which include real estate transactions.

Nationwide, the agency said, consumers lost $893 million in the past three years to fraudulent real estate transactions, and that's just among the 32,000 people who reported the scams during that time.

In most cases, the homeowner never sees the money again. And in most cases, the professionals working with the homebuyer — real estate agents, mortgage lenders, title companies and real estate attorneys — take no responsibility for the losses, which are

usually in the tens of thousands of dollars.

How can that happen? And is anything being done to stop it?

To make sense of it, it's essential to understand the anatomy of the scam.

THE ANATOMY OF THE SCAM

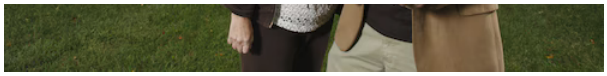
Real estate transaction scams are relatively simple.

The bad actors impersonate one of the professionals working on the sale. They create an email address that's substantially similar to the real one, but may be one letter off and easy to overlook. In more sophisticated cases, scammers hack into a professional's real email after stealing their login credentials from separate successful phishing attacks.

In one case profiled by Bamboozled, a couple lost more than $90,000 after a scammer created fake email addresses impersonating both their attorney and their real estate agent. The scammer also hacked into the buyer's Yahoo email address — probably linked to a data breach that affected 3 billion Yahoo accounts several years earlier.

The scammer was able to send emails across all the accounts while deleting the real ones sent by the agent and the attorney so the homebuyer would never see them.

And it worked.



Benjamin and Joyce Fox were the victims of an elaborate internet email scheme that ultimately cost them $91,500. In this 2017 image, they stand in front of the townhome in Lafayette they were in the process of buying when the online crime occurred. (Photo by Jerry McCrea for NJ Advance Media)Jerry McCrea

Even if the person who wired the money realizes the scam quickly, it's usually too late. The bad guy even more quickly takes the money that was wired. Once the money is gone, the bank will usually say there's nothing it can do.

SOLUTIONS?

Most real estate agents and attorneys warn their clients about these scams when they sign engagement letters. Some even have wire fraud reminders as part of their email signatures.

Some homebuyers, perhaps, never read the literature. But even if they do, they are still tricked by sophisticated impersonators while feeling pressure, urgency or even panic about transferring money for this life-changing purchase.

Indeed, when we recently wrote about this scam, we received many emails from consumers in New Jersey and across the country who were either victimized in a real estate fraud or who almost fell victim but caught it at the last moment.

Many were surprised to learn that while their professionals had liability insurance, some didn't have cyber-coverage and others said claims were denied because the imposter email addresses were not caused by the insured professional.

They all said real estate professionals — whether agents or title

companies or attorneys — need to do something to better protect their email communications.

Jessica Madalena sits on the front steps of her Wood-Ridge home. She and her fiancé lost more than $32,000 in a wire scam when they purchased their home.Courtesy Jessica Madalena

One had a good suggestion.

“A critical vulnerability was the unencrypted email communications between our realtor, the seller’s realtor, the title company, and the loan originator,” said Tim Olsen, a Texas victim who said he lost thousands in a similar scam.

In his case, the con artist added an extra “i” in the word “title” in an email address, and he didn’t catch it, he said.

Neither did anyone else, he said, noting the scam emails, which went to all the parties, contained copies of the full purchase contract, the financing details and the down payment amount.

Olsen said requiring encryption for all email communications between buyers and their professionals could be an answer.

“This simple step could prevent similar scams and protect countless families pursuing the American dream of homeownership,” he said.

Encryption, which protects data when it’s in transit, does provide

some protection, but it may not be enough, cybersecurity experts said.

Schemes like these were probably not pulled off by intercepting emails in transit, said David Opderbeck, a law professor and co-director of the Gibbons Institute of Law, Science & Technology at Seton Hall University.

“It’s much more likely that the scammers breached computer systems controlled by the consumer, the law office, or the real estate agent, to access stored data,” he said, noting that such stored data is called “at rest.” “Even if the sender had used end-to-end encryption when sending emails, the emails would have been decrypted when received, and therefore in plaintext when stored at rest.”

So what would help then is “full disk encryption,” which automatically encrypts all the data stored locally on a drive, he said.

But even that may not have prevented the attacks, he said.

“Phishing scammers often gain access to log-in credentials for email services, such as Microsoft 365 and Gmail, which store data in the cloud rather than on a local hard drive,” he said. “If the scammer is able to log in to the customer’s, lawyer’s, or real estate agent’s cloud-based email accounts, they will get access to plaintext data even if local hard drives are encrypted.”

Using a portal to share sensitive information — such as those that are commonly used by doctor’s offices to share information with patients — is another option. But that, too, isn’t foolproof.

“A portal in itself doesn’t protect against attacks on data at rest or

against attacks that employ stolen log-in credentials," Opderbeck said.

A centralized portal could present large-scale upheaval if a hacker takes interest.

"The moment you introduce a centralized platform, you're putting a high premium bullseye on the platform," said Stanislav Mamonov, an associate professor in the information and business analytics department at Montclair State University.

He cited the recent ransomware attack on a software system used by more than 15,000 car dealerships nationwide which caused disarray for weeks, and the attack on a health care payment system that disrupted health care services for months and netted the hackers $22 million in Bitcoin.

Meenal Gupte sits on the front steps of her Randolph home. She and her husband were scammed out of $25,000 in a transaction to purchase the home in 2022. The bank froze the money, but the couple still doesn't have the funds back 20 months later.Courtesy Saurabh Gupte

Mamonov said capturing the scammers is "a game of whack-a-mole."

He said the ease of electronic payments also creates ease for

cyber fraud, so it may make sense to consider low-tech solutions for this high-tech problem.

“One of the mechanisms would be to go back to old-school checks,” he said. “In order to deliver the payment, you would have to meet with the person you recognize. That would create less of an opportunity for cybercriminals to insert themselves in the transaction.”

WHAT THE INDUSTRY SAYS

The National Association of Realtors said it does not have any formal policy requiring the use of an encrypted portal.

But its code of ethics requires its members to provide services that “conform to the standards of practice and competence which are reasonably expected in the specific real estate disciplines in which they engage,” said Chris Christensen, director of technology policy.

He said members would have an ethical obligation to adopt encrypted portals when they become more commonplace.

Christensen said the group supports “enhanced procedures for furnishing wire transfer instructions to consumers, including the masking of a portion of the account number and the implementation of a mandatory call to obtain the remaining digits.”

The American Land Title Association, the trade association for the abstract and title insurance industry, said increasing awareness is a priority.

Diane Tomb, the group’s chief executive, cited a list of steps the group has taken to educate consumers, its members, real estate professionals and others in the industry, adding that it also updated its best practices to evolve with technology and wire fraud scams

and to encourage the use of wire verification services and multi-factor authentication.

The group had no comment specifically on using encrypted portals.

The American Bar Association said it did not have a policy on the issue.

THE LAW

To date, there has been no legislation introduced in Trenton to address these kinds of scams, according to the state Office of Legislative Services.

There is a measure calling for the Division of Consumer Affairs to launch a public information campaign about rental scams, but nothing that addresses home purchase scams.

The state Department of Banking and Insurance, in 2018, issued a bulletin about the "prevalence of fraudulent schemes to divert funds transferred by wire."

It hasn't published anything since but said the bulletin is still in effect.

This past April, New Jersey Office of Homeland Security and Preparedness' cybersecurity division issued an alert about the uptick in scams based on the FBI report that said New Jersey victims ranked second in the nation for the amounts stolen in these kinds of frauds.

So what's the answer?

Educational campaigns are a good thing, and consumers and real estate professionals alike need to be reminded of the risks.

But that's obviously not enough.

Perhaps requiring all participants in a real estate transaction to use a secure encrypted portal, while not foolproof, would be a start. Maybe forbidding email transmission of full account numbers for wire instructions could help.

Should everyone be required to hand-deliver paper checks and forget about wires altogether? That's not realistic.

What do you think? Is there a solution that lawmakers in Trenton can take up to protect consumers?

Send me an email with your ideas.

- Check your mailbox! The first round of Senior Freeze checks are on the way, state said.
- When will I get my ANCHOR benefit? The latest on N.J. property tax savings.
- They almost lost $25k in real estate scam. Why won't bank release their money?

Please subscribe now and support the local journalism YOU rely on and trust.

Karin Price Mueller may be reached at KPriceMueller@NJAdvanceMedia.com. Follow her on X at @KPMueller.

in accordance with our Privacy Policy.