How Cybercriminals are Targeting Real Estate Transactions

Scott H. Hogan
Foster Swift Finance Real Estate & Bankruptcy Law News
March 30, 2025

AUTHORS/ CONTRIBUTORS
Scott H. Hogan

PRACTICE AREAS
Business Contracts
Cybersecurity and Data Privacy
Real Estate Law
Technology Law

As you are finally getting ready to close on a dream real estate deal, you get an email from your mortgage broker with wire transfer instructions to get the deal done. Once the money is sent, the dream seems too good to be true. However, the dream can soon turn into a nightmare when you realize that you've been the victim of a costly crime.

While it may sound like the plot from a fictional police drama, this type of cybercrime has been on the rise in recent years. In fact, according to the Federal Bureau of Investigation (FBI), in 2022 alone, $446.1 million were lost to scammers that used fake emails about real estate deals. And it makes sense that cybercriminals would target real estate transactions: Large sums of money are involved, wire transfers allow criminals to get their hands on these funds quickly, and plenty of personal information is present to be exploited later.

Everyone involved in real estate transactions must proceed with caution: remaining hypervigilant can keep transactions safe from the prying eyes of cybercriminals.

How are Cybercriminals Exploiting Real Estate Transactions?

As cybercriminals are becoming increasingly sophisticated, they have developed multiple tactics for exploiting real estate transactions, including:

BEC scams. Business email compromise (BEC) scams occur when cybercriminals impersonate real estate agents, title companies, or brokers to ask for payments or change the terms of a deal. They may also commandeer an email account entirely, which not only gives them the opportunity to contact homebuyers and sellers, but also gain access to sensitive information.

Ransomware attacks. During a ransomware attack, criminals get into a company's data and lock it so no one in the organization can regain access. While the data is locked, cybercriminals will demand a high

ransom to provide a code that will open the system. In some cases, these attacks can take months to be resolved.

Wire fraud. This is the most common way that cybercriminals get access to funds in real estate transactions. Once they hack into an email account—which could belong to the buyer, seller, title company, or real estate agent—criminals will monitor messages until the time is right to strike. Then they'll send fake wire payment instructions to the homebuyer and collect the funds. Sellers may be vulnerable to this tactic too.

Strategies to Combat Real Estate Cybercrime

Although cybercriminals are constantly evolving their schemes, there are ways individuals and companies involved in real estate transactions can protect themselves, including:

Security measures. There are various cybersecurity measures that real estate professionals and consumers alike can use to protect themselves from hackers. For example, enabling multifactor authentication on all company email addresses can help keep messages safe and raise an alarm when someone who isn't authorized tries to gain access to them. Similarly, utilizing network security tools, such as firewalls and intrusion detection systems, are a companywide solution that further keeps data protected. Also, creating strong passwords for everything from email accounts to cloud-based systems make it more challenging for cybercriminals to penetrate an organization's systems. Also, any person who is wiring funds should call the recipient before sending the wired funds to confirm the recipient's identity and wire instructions.

Insurance. Getting cyber insurance is a great way for real estate professionals to prepare for when the worst happens. This helps organizations with expenses related to business interruptions, lost data, and legal issues that may arise after a cyberattack. Also, this can be helpful if title insurance does not cover cybercrime.

Education. No amount of protection will make a difference without education on the ways cybercriminals operate. Real estate professionals should educate their employees about the tactics hackers use and how to avoid falling victim to phishing schemes and other suspicious email activities. Also, clients can be advised on how to detect fake emails and encouraged to always verify any requests for money and changes to instructions.

When cybercriminals attack, real estate transactions can turn a joyous occasion for homebuyers and sellers into a traumatic experience. For information on how to prevent real estate cyber fraud, or deal with its aftermath, contact a member from Foster Swift's Finance, Real Estate & Bankruptcy Law and Cybersecurity practice teams.