

Uncovering a New Tactic in Real Estate Wire Fraud

Introduction

Wire fraud continues to be a significant concern for businesses, posing substantial financial and reputational risks. The ever-evolving tactics employed by fraudulent actors demand continuous vigilance and innovative countermeasures. This SAFE Alert discusses new Tactics, Techniques, and Procedures (TTP) for wire fraud that exploits the inundation of spam emails to deceive and defraud escrow officers. We will explore the key characteristics of this TTP and provide actionable strategies to mitigate the associated risks.

Characteristics of the New Technique

Here's how these new vacant property scams work:

- **Utilization of Spamming Techniques:** To set their deceitful plan in motion, fraudulent actors skillfully employ spamming techniques to register the escrow officer on countless mailing lists. By doing so, they flood the officer's inbox with an overwhelming number of spam emails, burying crucial information under a heap of digital noise.
- **Inundation of Spam Emails:** With the escrow officer unwittingly caught in the spamming web, they are bombarded with thousands of spam emails. These emails serve as a smokescreen to distract the escrow officer, making it harder to see any emails from the buyers questioning the new wire instructions.
- **Fraudulent Wire Instructions:** Capitalizing on the chaos caused by the deluge of spam, the fraudulent actor seizes the moment to send phony wire instructions to unsuspecting buyers. These instructions are designed to mimic legitimate ones, tricking the recipient into making unauthorized and potentially irreversible wire transfers.
- **The follow-on effect:** Even after the wire fraud event has been completed, the escrow officer will continue receiving more spam emails. This effect will continue for several days to weeks.

Mitigation Strategies

To protect yourself from falling victim to this scam and mitigate the risks associated with real estate wire fraud, we recommend the following strategies:

I. Email Vigilance

Remain vigilant when it comes to email communication. Scrutinize any emails that appear suspicious or out of the ordinary. Look for telltale signs of phishing attempts, such as misspelled words, grammatical errors, and unusual requests. If you suddenly receive a large number of spam emails (over 25), that red flag indicates fraudsters are preparing to attempt wire fraud on one of your transactions.



2. Raising Awareness

Educate yourself and others involved in real estate transactions about this spamming scam. Make sure escrow officers, consumers, and buyers are aware of the tactics employed by fraudsters. Encourage open and transparent communication between all parties to ensure everyone remains on guard against potentially fraudulent activities.

3. Ongoing Training and Awareness

Continuously update your knowledge about the evolving tactics used in real estate wire fraud. Stay informed about the latest scams, techniques, and best practices for security. Engage in ongoing training to sharpen your skills in detecting and mitigating potential threats.

4. Two-Factor Authentication

Multi-factor authentication is sometimes called two-factor authentication or two-step verification, and it is often abbreviated to MFA. No matter what you call it, MFA is a cybersecurity measure for an account that requires anyone logging into an account to prove their identity multiple ways. Typically, you will enter your username and password and confirm your identity by using an app or responding to a text message.

Why go through all this trouble? Because MFA makes it extremely hard for hackers to access your online accounts, even if they know your password.

It might seem like a lot of work, but once you set up your MFA, proving your identity usually adds just a second or two to the login process. And the peace of mind MFA provides is well worth it. Implement MFA for any account that permits it, especially any account associated with work, school, email, banking, and social media.

5. Secure Communication Channels

Whenever possible, utilize secure communication channels outside of email for essential discussions related to wire transfers. Utilize encrypted messaging platforms or secure document-sharing services to exchange crucial information. These alternate channels provide extra protection against interception and ensure secure communication with all involved parties.

Conclusion

Real estate wire fraud continues to evolve, and fraudsters are using increasingly cunning tactics, such as the spamming scam, to deceive unsuspecting individuals. By staying informed, remaining vigilant, and implementing the suggested mitigation strategies, you can protect yourself and your customers from falling into the hands of fraudsters. Remember, in the game of cybersecurity, knowledge is power, and taking a proactive approach is the best defense against these sneaky scams. Stay safe, stay informed, and keep those cyber-criminals at bay!

