SHINE BRIGHT

CYBERCRIME'S IMPACT ON THE REAL ESTATE INDUSTRY

Online criminals are targeting the real estate industry and stealing large sums of money from unwary homebuyers. This fraud can destroy real estate transactions, so the National Association of REALTORS® is urging real estate professionals across the country to immediately implement safety measures to reduce the risk of becoming a victim.

In a typical scenario, a criminal will hack into the email account of a person involved in an upcoming real estate transaction. The hacker will then send a sham email to the buyer, or another individual who will be wiring transaction-related funds. The email will state that there has been a last-minute change to the wiring instructions. Following the new instructions contained in the email, the recipient will then wire the money directly to the hacker's account, which will be cleared out in a matter of minutes. The money is almost always lost forever.

Most email users today can easily recognize the email scams that are rife with poor spelling and grammatical oddities. In contrast, the fraudulent emails being utilized in this wire scam are virtually indistinguishable from legitimate communications. Because hackers are gaining access to the email accounts of individuals directly involved in the transaction, they're able to include detailed information in their fraudulent emails, including key names, dates and mocked-up signature lines. There are a number of measures that real estate agents and others involved in real estate transactions can take to help keep themselves and clients from falling victim to this crime:

1

From the outset of any deal, inform all parties to the transaction of this scheme to ensure that everyone stays alert to suspicious activity.

2

Request that all parties implement reasonable security practices throughout the course of the transaction, such as only using confirmed telephone numbers or face-to-face communication to share sensitive financial or personal information.

3

Prior to wiring any money, the person initiating the wire should call the intended recipient via a verified telephone number to confirm the wiring instructions.

Other important steps to avoid exposure to email fraud include:

- Never conduct business over unsecured WiFi.
- Clean out email accounts on a regular basis.
- Change email passwords on a regular basis.
- Implement complex passwords with a combination of letters, numbers and special characters.
- Implement the most up-to-date firewall and anti-virus technologies.

If a fraudster has successfully infiltrated a transaction, NAR recommends the following steps:

- If money has already been wired via false wiring instructions, immediately call all banks and financial institutions that could possibly put a stop to the wire.
- Contact your local police.
- Contact all parties who may have been exposed during the attack so that they take appropriate action.
- Change all passwords.
- Report activity to the FBI's Internet Crime Complaint Center.

This advice is not all-inclusive, and real estate professionals should work with information technology and cybersecurity professionals to ensure that their email accounts, online systems and business practices are as secure and up-to-date as possible.

HELPING YOU SHINE BRIGHT