CYBERSECURITY

12 TIPS TO PROTECT YOURSELF & PROTECT YOUR CLIENT.

In recent years, real estate professionals have reported an upswing in a particular wire scam. A hacker will break into a licensee's e-mail account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a close, the hacker will send an e-mail to the buyer, posing either as the title company representative or as the licensee. The fraudulent e-mail will contain new wiring instructions or routing information and request that the buyer send transaction-related funds accordingly. Unfortunately, some buyers have fallen for this scheme and have lost money.

Two possible red flags to be aware of and alert clients to are any reference to a "SWIFT wire" transaction and terms that indicate an overseas destination for the funds. However, unlike many other e-mail-based "phishing" schemes, this particular manifestation appears to be more sophisticated and less recognizable as fraud. The communications do not contain the typical grammatical or stylistic oddities that are often present in scam e-mails. In addition, because the hacker has been monitoring the licensee's e-mail account, the fraudulent communication may include detailed and accurate information about the real estate transaction, including existing wire and banking information, file numbers, and key dates, names, and addresses. Finally, the e-mails may come from what appears to be a legitimate e-mail address, either because the thief has successfully created a sham account containing a legitimate business's name or because they are sending the e-mail from a legitimately hacked account

Be aware that this particular scheme is only one of many forms of online fraud perpetrated against real estate licensees and their clients. In protecting all parties to a real estate transaction from cybercrime, here is some advice for you and your clients to protect yourselves from becoming a victim of wire fraud::

1. Never send any sensitive financial information via e-mail without encrypting it.
2. Insist all parties on the transaction to have security measures in place.
3. Never conduct business over unsecured public wifi available at your local coffee shops and hotels.
4. Prior to wiring any funds, you should contact the intended recipient via a verified telephone number and confirm that the wiring information is accurate. Do not rely on telephone numbers or Web site addresses provided within an unverified e-mail.
5. CTC does not accept emails from Gmail, Yahoo, or AOL since they are not secured emails.
6. Our company does not take any direction from Buyers or Sellers directly, everything goes through the escrow team, and we call and verify by phone to make sure any changes that we may have received by email are correct.
7. Clean out your e-mail account regularly. Your e-mails may establish patterns in your business practice over time that hackers can use against you.
8. Change your user names and passwords on a regular basis.
9. Never click on any links in an unverified email. In addition to leading you to fake websites, these links can contain viruses and other malicious spyware that can make your computer – and your transactions –vulnerable to attack.
10. Trust your instincts. Tell clients that if an e-mail or a telephone call ever seems suspicious or "off," that they should refrain from taking any action until the communication has been independently verified as legitimate.
11. Make sure to implement the most up-to-date anti-virus software installed on your computers.
12. Provide a copy of this article to everyone on the transactions.

CTC of California
Consumer's Title Company