Buying a home? Watch out for mortgage closing scams

By Davida Farrar – JUL 07, 2017

Summer is a busy homebuying season. If you're in the market for a new home this year, watch out for email phishing scams. According to reports, the scams target homebuyers who are nearing the closing date on their mortgage loan. The scammers attempt to steal the homebuyer's closing funds—for example, their down payment and closing costs—by sending the homebuyer an email posing as the homebuyer's real estate agent or settlement agent (title company, escrow officer, or attorney). The email falsely

claims there has been a last minute change in the closing process, for example, that a check is no longer acceptable or that the wiring instructions have changed. It instructs the homebuyer to wire or otherwise electronically transmit the closing funds to an account that the scammers control. The Federal Trade Commission (FTC) warned homebuyers of this scam in blogs in March 2016 and June 2017.

We encourage consumers to exercise vigilance and caution to proactively guard against these scams. Below are some tips, including tips from the FTC, Financial Crimes Enforcement Network (FinCEN), and the FBI, to help you protect yourself against these types of phishing scams and take action if you are a victim.

Avoid email phishing scams

Phishing is when internet fraudsters impersonate a business to trick you into giving out your personal information. **These tips may help homebuyers avoid this type of scam.**

- Discuss the closing process and money transfer protocols with your real estate or settlement agent.
- If you receive an email requesting that you send money in connection with closing, even if it's from a familiar source, STOP. Call your real estate or settlement agent to discuss. **Don't use phone numbers or links in the email.**
- Don't email financial information. Email is not a secure way to send financial information.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain malware that can weaken your computer's security.
- Before sending any wire transfer, ask your bank for help identifying any red flags in the wiring instructions. Red flags include potential discrepancies between the account name and the name of the intended beneficiary (i.e., your real estate or settlement agent). Your bank may also be able to compare the receiving account number to account numbers identified in past consumer complaints as the destination of fraudulent transactions.
- Confirm receipt of the wire transfer by your real estate or settlement agent a few hours after the wire was transmitted. If you or another entity involved in the closing suspect a problem, report it to law enforcement and your bank as soon as possible to increase your likelihood of recovering the money.

What to do if you are a victim

- Contact your bank or the money transfer company immediately upon discovering that funds have been transferred to the wrong account. Ask the bank or money transfer company to attempt a wire recall.
- Contact your local FBI and state Attorney General office.
- File a complaint, regardless of the dollar amount, with the FBI's Internet Crime Complaint Center at www.ic3.gov. Part of the mission of ic3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity. Information is analyzed and used for investigative and intelligence law enforcement purposes and for public awareness.
- Report the phishing scam to the FTC.
  The FTC and the FBI have more information on protecting yourself from phishing scams and what to do if you are a victim.