Business email fraud is a sophisticated scam that targets employees of a business to transfer money to criminals. Business email fraud is responsible for $1.6 billion in losses in the U.S. and $5.3 billion globally since 2013. The FBI reports that business email fraud has increased 2,370% since 2015. During the second half of 2016, the FBI received over 3,000 reports with losses totaling $346 million.

One of the most popular industries to target for email fraud is real estate. A real estate transaction involves many professionals, such as real estate agents, financial institutions, brokers, and escrow or title agents. All of these professionals have emails that could be a potential point of entry for criminals. Business email fraud for the real estate industry is typically a four-step process:

1. Hackers can simply find a real estate agent’s email account on their websites, purchase email extractor software from the Internet, then use it to collect email addresses for thousands of people working in the real estate industry, or they can purchase the credentials of 10,000 real estate agents for around $11.
2. Hackers then send a phishing email that tricks the recipient into clicking on a link or opening an attachment. They only need one person to take the bait.
3. Once inside the victim’s email account, they can conduct extensive research on thousands of listing addresses, sales prices, loan amounts, escrow and title company information, and account numbers.
4. Criminals use this information to send an email that looks legitimate from the realtor, broker, bank, or title company’s email to the homebuyer instructing them to reroute funding from their lender to a new fraudulent account.

Fraudsters can even alter the signature block on a real estate contract to list a number that connects directly to the bad guys. So, if a homebuyer is suspicious and calls the number listed to verify this new account information is correct, the bad guys answer the call and confirm the fraudulent process. It only takes between 4 and 24 hours for a homebuyer’s life savings to disappear.

Tips for Businesses:
• Be careful about what you reveal about yourself and your company on social media channels and corporate websites.
• Be suspicious of requests for secrecy and to take immediate action.
• Implement a two-factor or multi-factor verification system to keep the bad guys out of your corporate email system.
• Utilize digital signatures and encrypt messages on both sides of the transaction.
• Don’t open unsolicited or spam email from unknown parties.
• Keep your company’s antivirus protection up-to-date and install all recommended service patches.
Tips for Homebuyers:

- Don’t trust any email that requests you to send money or wire funds to a different account.
- Follow up with a phone call to your original contact to verify the message’s authenticity.
- If you discover that you have transferred funds to a fraudulent account, contact your financial institution immediately and ask for a wire transfer recall. Be sure to state that you are a victim of business email fraud. Because you personally ordered the transfer to the fraudulent account, financial institutions consider the transaction to be legitimate.
- Notify the FBI, who will work with the U.S. Department of Treasury Financial Crimes Enforcement Network, to help return or freeze the funds.
- Fill out a Complaint Referral Form through the Internet Crime Complaint Center, identifying the incident as a business email fraud.

Source: Fraud of the Day - Business Email Compromise Fraud Matters

For more information or to file a complaint, contact Pinellas County Consumer Protection at (727) 464-6200 or visit www.pinellascounty.org/consumer.