Issued 7/20/18

BEC Scams and Real Estate Deals: How to Protect Yourself

Despite constant warnings by law enforcement and industry organizations, BEC scammers continue to fleece companies. They target small, medium, and large business and personal transactions, but have, in the last few years, shown a notable predilection for targeting companies in the real estate sector.

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a type of scam targeting both businesses and individuals performing wire transfer payments, and often starts with the attackers compromising legitimate business e-mail accounts. Once scammers have had enough time to analyze the contents of a compromised account, they usually have enough information to write a convincing/legitimate-looking email to the next target. The goal is to trick those targets into transferring funds to an account controlled by the scammers or into sharing personally identifiable information or wage and tax statement (W-2) forms for employees.

The real estate twist

The scammers target all parties in a real estate transaction: title companies, law firms, real estate agents, buyers and sellers. “BEC/EAC actors will use information that is publicly available on real estate listing sites to target victims. This may include homes that are for sale and the progress of the sale such as ‘under contract’ as well as the contact information of the real estate agent,” the FBI warns. In the spoofed emails, the scammers instruct the recipient to change the payment type (e.g., wire transfer instead of check dispersal) and/or payment location to a fraudulent account.

Protect yourself

“The best defense is to verify all requests for a change in payment type and/or location. Be wary of any communication that is exclusively e-mail based and establish a secondary means of communication for verification purposes,” the FBI advises. It is perhaps best to contact the sender of the email via phone and check whether they have actually sent that email or not, but be sure you’re not using the phone number provided in the email, as it might be that of the scammer.

The FBI also warns that scammers are also reaching out to targets via phone, requesting personal information for verification purposes. Financial institutions get phone calls acknowledging a change in payment type and/or location. Some victims said that they were unable to distinguish the fraudulent phone conversation from legitimate conversations, so the FBI advises establishing code phrases that only the two legitimate parties can know.

For those who fall for the scam, a quick reaction is essential: they should contact their financial institution and request a recall of the funds, then notify the FBI and report the fraudulent transfer. The funds are usually directed to a fraudulent domestic account which quickly disperse through cash or check withdrawals. The funds may also be transferred to a secondary fraudulent domestic or international account. Funds sent to domestic accounts are often depleted rapidly making recovery difficult.