BEC Scams

Today's topic is: Did you know? Business Email Compromise

The FBI released a public service announcement that Business Email Compromise (BEC) scams are on the rise. The total value of funds redirected as a result of BEC scams have topped $12 billion and the Internet Crime Complaint Center reports a 136% increase in identified global losses between December 2016 and May 2018.

The scams are continuing to evolve, targeting small, medium and large businesses as well as personal accounts reported in all 50 states and 150 countries. Based on reports, BEC scams are targeting the real estate market hot and heavy. Statistics show an 1,100% rise in the number of reporting victims and an almost 2,200% rise in monetary losses between 2015 and 2017.

Asian banks located in China and Hong Kong remain the primary destination of the fraudulent funds, however other countries are beginning to see more activity.

So, how does it happen? Scammers compromise a legitimate account via malware or phishing attacks and use it to conduct unauthorized transfers of funds or to direct others within an organization to do so. For example: when the CEO isn't in the office, the fraudster acting as the CEO will instruct the CFO to wire funds to an account immediately. Sometimes the scam is conducted using an email with a domain that closely matches the business, such as "abc_company.com" versus "abc-company.com".

Another scenario that might occur is: the fraudster poses as a legal entity and contacts a business regarding an "important matter." This can be done over the phone or email, and typically pressures victims into wiring money immediately and/or secretly.

In the real estate market, victims most often report a spoofed email either sent or received by a title company, law firm, real estate agent, buyer or seller with instructions to change the payment type and/or location to a fraudulent account. The funds may be directed to: A) a fraudulent domestic account which quickly disperse through cash and check withdrawals, or B) a secondary fraudulent domestic or international account.

Domestic money mules are groomed by the fraudulent party through confidence or romance scams into opening accounts to send or receive the fraudulent funds.

The following activity may be red flags or indicators of BEC:

- A communication that is exclusively email based or seems urgent or out of the ordinary.
- A poorly crafted email, an email with an incorrect email signature of the supposed sender or the use of full names and formal language structure that may be atypical.
- Transfer requests are communicated at a corresponding time the senior official is out of the office.

- A large funds transfer or wire is being sent to a recipient the business has not dealt with in the past.
- The transfer is requested near the end of day or right before the weekend or holiday.
- The funds are being sent to a personal account when the company typically only sends wires to businesses.
- The receiving account shows no prior history of large funds transfers.

Lessen your chances of becoming a victim by keeping the following tips in mind:

- Be wary of any communication that is exclusively email based or seems urgent or out of the ordinary. Establish a secondary means of communication for verification purposes.
- Craft a policy for identifying and reporting BEC and similar email scams.
- Be mindful of phone conversations and the information you provide.
- Establish procedures when processing legal documents requiring any changes in payment type or location to be verified prior to distributing funds.
- Educate internal staff and key financial officers on BEC.
- Implement filters are your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- If you discover a fraudulent transfer, act timely. Contact your financial institution immediately. Contact your local FBI office and report the incident. File a complaint with www.ic3.gov or bec.ic3.gov.

Stay safe out there, folks! If you have any questions or concerns about how you can protect yourself or your organization against payments fraud, please reach out to us.

www.epcor.org