Beware of Business Email Compromise

One of the most convenient forms of communication can also be the most unsecure for a business if the proper channels and guidelines are not established and followed. Many companies—large and small—have fallen victim to scam artists. The invention of the internet, email and connected devices has only made it easier to attack businesses from afar, and it is only getting worse.

Business Email Compromise (BEC) is a type of fraud that is costing American businesses millions of dollars per year. On a global scale, it cost companies more than $5 billion between October 2013 and December 2016, according to the Federal Bureau of Investigation (FBI). The name of the scam speaks for itself, but there are a few different ways it can be carried out by a fraudster.

Typically, a spoof email address is created. This can be done by changing the format of the business' legitimate email; e.g., JohnSmith@business.com to JonSmith@business.com. The criminals can also take control of executive email accounts and ask for a wire payment. Small- and medium-size business can be hit the hardest since "they are often less likely to prepare for or recover from such a scam," said the FBI.

Last year in Virginia, there were more than 400 cases reported to the FBI's Internet Crime Complaint Center (IC3), totaling over $7 million in losses. So far this year, BEC has resulted in $40 million in losses in Phoenix, AZ, according to television station KVOA in Tucson. The IC3 has seen actual and attempted BEC losses over the last two years increase by more than 2,000%. It has affected all 50 states and more than 130 countries.

"Cyber risks can seem overwhelming in today's hyperconnected world, but there are steps you can take to protect yourself and reduce your risk," said FBI Cyber Division Assistant Director Scott Smith in a release. According to *Engineering News-Record*, there are four steps to follow:

- Know what you have to defend.
- Know how to detect bad things.
- Develop and test an incident response plan.
- Recovery—keeping the lights on.

This can be done by having a plan or a set of rules in place to avoid BEC altogether. Several NACM members said they do not allow financial transactions to be initiated by email, helping to prevent an executive-account takeover through which funds are requested to be transferred via wire immediately. A bit of common sense can also assist in dodging BEC.

The FBI suggests "carefully scrutinizing" emails and to be suspicious of a quick response time. Blindly abiding to the request can be a business' downfall, which is why it is important to "confirm requests for transfers or funds by using phone or in-person verification as part of two-factor authentication," the FBI noted. "The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone," said Special Agent Martin Licciardo in an FBI release. "Don't rely on email alone." Knowing your customers and their habits can also help avoid the scam. A change in business practices can be a red flag and cause questions to be raised.

Unfortunately, not all BEC can be stopped. If you become a victim, it is important to act quickly. "Delays in reporting the scheme make it difficult to stop wire transfers and recover any lost assets," the FBI

explained. It advises contacting your financial institution, the financial institution of the fraudulent transfer, the FBI and the IC3. “BEC is a serious threat on a global scale … and the criminal organizations that perpetrate these frauds are continually honing their techniques to exploit unsuspecting victims,” Licciardo said. This is why the first step of avoiding BEC is to know that it exists and anyone can be affected.