Three Best Practices to Prevent Business Email Compromise

By Trever Campbell, *Senior Manager*

In my last blog article, I shared with you "Three Things to Look for In Fraudulent Emails" related to business email compromise (BEC). This time we are going to continue that conversation and talk about three best practices you can put in place to help protect your organization.

It is no longer a question of if your organization will experience some form of BEC, it is now only a question of how frequently it will occur and how prepared you are to handle it. There are many things you probably already have in place in some way including: qualified IT resources or staff, firewalls, and antivirus software (make sure to patch and/or update your software regularly or it will be of very little use), but what I want to talk about today is lower hanging fruit than even those. Some of the best protection methods are also simple. Here are three best practices to prevent compromised emails within your business.

1. Educate employees – Like many things in life, prevention starts with education. To avoid the pitfalls inherent in BEC you need to prepare staff for what to expect. Don't assume they know what to look for or that fraudulent emails will be obvious and easy to ignore. Share the tips from the last article and discuss what your organization may have already experienced in the past. Training should be both mandatory and continuous. Upon being hired and once a year at a minimum they should receive refresher information as well as what new things to be on the lookout for. Many organizations use third-party services that send out fake fraudulent emails to test their staff's alertness. An important note on that type of activity is that you want to provide education, not discipline, if mistakes are made. The goal is the develop employees into partners in fraud prevention, not to be punitive. Encourage a culture where everyone is looking out for the best interests of the company and feels comfortable admitting when mistakes are made.

2. Protect sensitive information – The foundations of fraudulent emails are often built on real information. Fraudsters use social engineering to gain access to information that people assume could only come from inside the organization, therefore lending credibility to an otherwise unusual request. Be cautious about what information you make readily available to anyone outside your organization. Don't assume that sensitive information is simply financial in nature. Posting employee emails, phone numbers, and titles on the organization's website or social media accounts may make you more accessible to customers, but it will also make you more accessible to fraudsters. Know that if you do that you will need to be even more prepared for an eventual influx of fraudulent contacts. Even knowing when a certain person is on vacation can allow a fraudster to time an attack more effectively by either citing information that is assumed to be private or by targeting a less experienced replacement filling in on their job duties.

3. Low-tech verification – We discussed this some in the last article, but it's worth noting again. Sometimes the best solutions are old fashioned solutions. If an email appears potentially fraudulent, pick up the phone to confirm or verify. But now let's take it a step further and build that into some of the normal internal control processes as well. Before a wire transfer can be changed or finalized, create a two-step verification process that requires both a transfer number verification and a phone call with the intended recipient before the funds are released. Before a vendor's bank

routing information can be updated, require verbal confirmation that the request came from a known contact and that the newly provided information is accurate.

All three of these practices are relatively simple and inexpensive to implement. More importantly, just working on these efforts will increase the culture of fraud awareness in your organization, and in the long run that will go further than any individual control ever can toward preventing fraud.