BEC Still a Threat; Awareness and Training Key to Avoiding It

Published January 12, 2017

Business email compromise (BEC) is a form of phishing that targets specific people within a business by impersonating an executive or other person that may do business with the organization. As the name suggests, it's a scam using email messages in the hope that the recipient will not check for authenticity before performing a requested task. According to the FBI, costs to businesses because of BEC have exceeded $3 billion and that number continues to rise. The FBI has received complaints about this type of fraud from victims in every state in the U.S. and in at least 79 countries. It affects organizations of all sizes and does not discriminate based on industry or sector.

No matter how many technical security tools are in place, they will not keep 100% of phishing email out of anyone’s in box. Awareness and education will always be necessary. That’s because 30% of the recipients targeted for phishing actually open the messages, per Verizon. Unfortunately, Verizon also found that 12% of them actually click on malicious links or attachments.

Fortunately, there are some ways to avoid becoming a victim of phishing and BEC:

1. Did You Expect the Link: Always be wary of links or attachments that arrive in email messages that are *not expected*. Regardless of who the sender appears to be, it may not actually be that person. Email addresses are easy to fake, so if you receive an unexpected email that asks you to click something, take an extra second to check the entire email address in the header. Even then, it may not be safe so always use caution. If the email address of someone@company.com isn’t familiar; it could be trying to hook you.

2. Check the Link Destination: If you want to do an extra check of a link, hover over it with your mouse to see where it goes. If it doesn’t go where you think it should, it could very well be a fake and you should not click it. If you’re on a mobile device, you can hold down on the link for a few seconds to see the entire link. Just be careful to hold it long enough so that you don’t accidently click it.

3. Grammar and Spelling Mistakes: Although these are found less often now, if there are spelling or grammatical mistakes, it should be considered suspicious. Most companies are protective of their brand, so if it legitimately comes from a company with which you do business, it shouldn’t be riddled with mistakes.

4. Urgent or Threatening Language: If the email uses language that makes it sound threatening or urgent, take some extra time to evaluate it. Often, those committing BEC will make it appear as if it’s extremely important that an employee wire money right away. They also may use threatening language like “your account has been suspended” to get your attention. Don’t fall for it.

5. Verify Financial or Sensitive Information Requests: Take a moment to verify any request for a transfer of money or to send sensitive information via email. If the CEO is asking for a large payment or transfer for example, call him or her on the phone or send a separate, new email messages to confirm. If it is a scam, they will be thankful you took that time.

6. No One Needs Your Credentials: Never give out credentials for financial accounts to anyone. No one that truly has access should need yours.

7. Verify, Verify, Verify: If you suspect something is amiss, contact the sender separately using contact information you already have and know is safe or by looking it up independently of the email message. Scammers will often put contact details in email messages that just go right back to them.

Finally, be aware of the information shared on social media and networking sites. Anything shared on the Internet, regardless of how secure you think your social media or networking page may be, should be considered publicly available. While this may be great if you’re looking to make business contacts, it’s not great if the information is used to scam you.