Three Things To Look For In Fraudulent Emails

By Trever Campbell, *Senior Manager*

Since the start of COVID organizations have seen a significant increase in fraud and fraud attempts. A study by the ACFE (Association of Certified Fraud Examiners) shows that 51% of organizations have seen an increase in fraud uncovered since the start of COVID and that 71% expect to see an even greater increase in the coming year. Leading the way amongst all current fraud trends is cyberfraud, where an 82% increase is predicted in the next 12 months, and one of the biggest players in cyberfraud is business email compromise (BEC). At this point the only people who have not experienced any form of BEC are those who still use handwritten correspondence exclusively. It's safe to assume that if you have an email address, at some point you have received a fraudulent message trying to scam you out of money or information. Below are three things to look for to spot a fraudulent email.

1. Check for spelling – Fraudulent emails are not always easy to spot. We all like to think that we are too smart to be tricked, but many of them are very convincing. One thing that often gives them away is simply a misspelling within the email or email address itself. I recently received an email indicating that my Microsoft 365 account had "Unusual sign-in activity". Everything about it looked legitimate, and like many similar emails I had received in the past, including the link to "Review recent activity". The one thing that gave it away was that it came from an email account "security@micra-soft.com". The spelling of Micra-soft vs. Microsoft was not immediately obvious as I had to hover over the sender to see the account domain. Taking a moment to analyze the email for spelling or other fundamental errors could save you countless hours of headache and potential financial loss later, which leads to the next tip.

2. Don't fall prey to urgency – There are few, if any, emergencies we will face in life that will be communicated to us exclusively through email. However, that is exactly the feeling fraudulent emails will try to convey. Your boss needs you to send them a wire for $50,000 dollars *now*! Your account has been compromised and you need to change your password *immediately*! The IRS has been trying to contact and this is your final notice. If you want to stay out of jail you need to *reply back with 24 hours!* If you are reading an email and find yourself feeling hurried, rushed, or uneasy, that is exactly the time to slow down. Allow yourself the opportunity to think clearly for even a few minutes, and you will typically then be able to hear that voice in the back of your mind that says, "wait a minute… this doesn't make sense."

3. Unsolicited links and files – Another common technique used in BEC, that pairs with the sense of urgency, is an attached file you need to review right away, or a link to more information. Think about the example above with a link to review my recent activity. Or you may have received a file of an invoice that needs your approval or else you will be charged. Many of these emails are call phishing attempts for a reason. The email is just the line, mostly inert unless you interact with it. The file or link is the hook, and once you engage with it you are well on the way to being defrauded. If you receive an email that you are not expecting with a link or file attached do not engage with it right away. Instead pick up the phone and call the sender using a number that is not included in the email itself. If it looks to have come from someone you already know call them from their historical

phone line. If it comes from someone you are not familiar with, search for their contact information through their organization's website (again, not from a link in the email).

Now that you know some things to look for, stay tuned. In the next blog we will be following up with three best practices you can put in place to help your organization with even better BEC prevention.