MILNER

How to Prevent a Business Email Compromise Attack

Did you know?

Business Email Compromise (BEC) is one of the most common threats today. It employs tactics like impersonating an executive, HR, or a trusted vendor to initiate fraudulent transfers of money. According to the FBI, $1.7 billion was lost to BEC in 2019 alone.

Here are tips from the FBI to stay secure:

- **Be Skeptical**
  Last-minute changes in wiring instructions or recipient account information must be verified.
- **Don’t Click It**
  Verify any changes and information via the contact on file—do not contact the vendor through the number provided in the email.
- **Doublecheck That URL**
  Ensure the URL in the email is associated with the business it claims to be from.
- **Spelling Counts**
  Be alert to misspelled hyperlinks in the actual domain name.
- **It’s a Match**
  Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender’s email address appears to match who it’s coming from.
- **Pay Attention**
  Often there are clues with Business Email Compromise:
  - An employee who does not normally interact with the CEO receives an urgent request from them.
  - You see data that shows an employee is in one location at 1:00pm but halfway around the globe 10 minutes later.
  - You see activity from an employee who is supposed to be on leave.
- **And, As Always, if You See Something, Say Something**
  If something looks awry, report it to your MSP or a supervisor. And if you have been a victim of BEC, file a detailed complaint with www.ic3.gov.

Make sure you’re providing ongoing education to your customers’ end users to keep them secure.
Use this checklist as a leave-behind with your customer. They can print it out and post it next to all workspaces.