Toolbox Series:
Avoiding Email Compromise

By Jason Preu, VP, ISO, Information Systems and Security Manager, Bank of Labor

Email Compromise is a type of scam targeting almost any company or organization that uses email. Often, the credentials for corporate or publicly available email accounts of high-level employees in finance or involved with authorizing payments are compromised through phishing attacks. The attacker's goal is to then use the stolen email credentials to initiate fraudulent transfer requests. This can result in hundreds of thousands of dollars in losses.

Scammers impersonate executives authorized to transfer money. In addition, fraudsters also carefully research and closely monitor their potential victims and their organizations, often observing a target's mailbox for months.

E-mail compromise scams have resulted in organizations losing billions of dollars. As sophisticated as the fraud is, however, there is an easy solution to help thwart it: face-to-face or voice-to-voice communications. Verify the authenticity of e-mail requests to send money by talking with the CEO's in office or calling back the person allegedly making the request on a previously known number.

"Shark Tank" star, Barbara Corcoran, has recently become a victim of this scam. The scam started last week when an email chain was forwarded to Barbara's bookkeeper, a woman named Christine.

The email appeared to have been sent from Barbara's executive assistant, Emily, and it informed Christine she needed to pay $388,700 dollars to a company called FFH Concept GmbH (a real company) in Germany.

The problem is that email didn't really come from Emily. The scammers changed Emily's email address by removing one letter, so they were the ones actually communicating with Christine.

Christine followed-up on the request via email by asking fake Emily all the right questions. She even got an email back with the perfect cover story that explained everything. Satisfied, the bookkeeper fired off the wire to the account requested.

Afterward, she emailed the real Emily -- at her real email address -- and it was only then that they uncovered the scam because real Emily noticed her address was altered on the previous chain of emails.

Moral of the story: Had Christine called Emily back, instead of only trusting the email, the scam would have been averted.

Email is an amazing communication tool. It is, however, fundamentally broken as a sole source of trusted information. Always verify unsolicited requests.

Bank of Labor
BORN OF INTEGRITY