Published on *The National Law Review* https://natlawreview.com

Emails That Do Not Make Your Spidey Senses Tingle Can Lead to Huge Losses

Article By:

Michelle L. Dama

Adrienne S. Ehrhardt

Nancy Leary Haggerty

You just received an email request from your boss who is out of the office but needs you to email him sensitive employee files because he is working on a confidential matter that cannot await his return. Or, you are a title company handling a real estate closing, and the seller just emailed you wire instructions from her personal email account directing you where to deposit proceeds from the sale of her home. Neither of these emails raises immediate suspicion because there are elements to them that sound familiar to you. You personally know the person requesting action, or the requestor demonstrates familiarity with the transaction or certain business protocols. So, you do your job. It turns out that you replied to a fraudulent email and just sent a trove of sensitive personal information out the door and wired hundreds of thousands of dollars to wrongdoers.

Business email compromise (BEC) scams are on the rise. These low-tech but socially sophisticated cyber-attacks rely on spear-phishing emails that appear to be from someone you know, often an executive or someone in senior management, requesting money or sensitive employee records. They generally request immediate action and commonly contain the terms “Urgent,” “Request,” or “Payment” in the subject line. In its April 2017 Internet Security Threat Report, the security solutions company Symantec identified BEC scams as one of the top growing cybersecurity attacks this year. These compromises have grown at an alarming rate. Between January 2015 and December 2016, there has been a 2,370% increase in BEC scams with a total combined loss of over $5 Billion in the last three years.

Cyber-attackers use social engineering to lure employees and individuals into believing that they are responding to legitimate requests. They may even hijack genuine invoices sent by real companies and only change the account number to the hacker’s account number to successfully receive payment. These attacks have been lucrative and have the potential to snare sophisticated individuals. In January 2016, the CEO of an Austrian aerospace company was involved in a BEC scam that resulted in the transfer of $47 million, which essentially wiped out most of the profits for the company that year. Cyber-attackers not only seek cash but also personal employee information. The Milwaukee Bucks fell victim to this when an employee responded to an email from someone posing

as the Buck's President and sent scammers the W-2 information for its players, which included name, address, Social Security Number, and compensation information. No industry seems to be immune to BEC scams, but they are fastest growing in the finance, insurance, and real estate space.

In the real estate arena, the scams typically involve the identification of real estate professionals (realtors/brokers/title agents) that have a high volume of incoming wire transfers. Hackers gain access, monitor the business email accounts, and intercept legitimate funds requests and transfer instructions. The hacker then modifies the instructions to direct the funds to a fraudulent account. The client then wires the funds for the real estate purchase to the fraudulent account.

The following are some best practices to protect against BEC scams:

- Raise awareness of BEC scams within the organization or early in a transaction; a greater understanding of potential attacks raises the potential for employees and individuals to recognize when they are being targeted by fraudsters.
- Avoid using and responding to emails from free web-based email accounts.
- Be suspicious of requests to act quickly, secretly, or without following usual procedures.
- Confirm any changes to wire transfer information verbally.
- Draft a separate reply to the email sender to a known email address rather than hitting the Reply button
- Do not give out sensitive information via email.
- Have a second out of band communication channel to verify transactions for significant amounts of money, such as a telephone call using a previously known telephone number, or other previously agreed upon communication method that is not one suggested in the email request itself.
- Be careful in posting information about executives or employees on social media or company websites that provides detailed job duties, hierarchical information, and out of office details such as vacation schedules; BEC scams often coincide with business travel or vacation dates.

National Law Review, Volume VII, Number 129