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

As Reports of Hacking and Wire Fraud/BEC Scams Increase, Here's What you Can Do to Prepare

Article By:

Basileios "Bill" Katris

Business Email Compromise ("BEC") is a scam perpetrated by cyber criminals to attack businesses that first began to be tracked and reported by the FBI in 2013. BEC typically consists of phony or phishing emails that appear to originate from a company executive or member of a company's accounting or finance department containing fraudulent payment instructions with the objective to direct or redirect business funds to the cyber criminals. Cyber criminals are targeting all sizes of business, from small to publicly traded and any size in between.

DRAMATIC INCREASE IN LOSSES - ILLINOIS IN TOP 10!

In 2018, annual losses due to the BEC Scam more than doubled to $2.7 billion. According to the FBI, since 2015 these losses have increased more than 1,300 percent. As reported by the FBI in April 2019, Illinois made the “Top 10 States list” for both number of victims and total average loss by victims. Mimecast reported in its 2019 “State of Email Security” report that BEC attacks increased by 67% over last year, with 73% of victims incurring a direct loss.

WHAT YOU NEED TO KNOW

BEC scammers are gaining sophistication in their tactics and techniques, which often monitor an intended target's email systems to hack accounts, limit detection and perfect the timing of their fraud to go unnoticed. These schemes are going on for longer periods of time with a substantial investment of time by the cyber criminals in order to ensure a successful crime and larger pay day. The FBI has noted that these cyber-criminal organizations are now employing linguists, lawyers, accountants and other professional service providers to infiltrate and implement their schemes. It is important to note that a traditional data breach is not necessary for a BEC scam occur. The scam is typically implemented in a combination of one or all of the tactics below:

- **SPEAR-PHISHING**: fake emails from a purported trusted sender seeking the disclosure of confidential information
- **MALWARE**: used to access business networks in order to gain access to legitimate e-mail threads about billing and invoices. Malware later leads to the spoofing of email accounts and theft of funds

- **SPOOFING OF EMAIL ACCOUNTS AND WEBSITES**: when a criminal sends an email that is a slight variation of a legitimate address (doe@xyzcompany.com vs. john.doe@xyzzcompany.com) that fool victims into thinking fake accounts are authentic. The criminals then employ a spoofing tool to direct e-mail responses to a different account that they control. The victim thinks he is corresponding with a trusted person only later to find out that is not the case. *Many times the criminal sends the spoofed email in the midst of an ongoing transaction and so the victim's awareness is low thereby allowing the crime to occur*

PREVENTION

Here are some tips to implement internally that might help prevent, limit or mitigate the damage done by BEC:

- Alert each employee in the payment process chain that payments must be verified with unique measures
- Confirm any payment change requests verbally and in detail as to new account numbers from known parties
- Procure the right amount & type of cyber crime insurance
- Use contracts to limit liability
- Consider employee training for payment transactions
- Properly secure your email and IT systems from cyber-attacks and employee carelessness
- Send reminder emails to all business partners that any requests from your business to alter payment methods must be verbally confirmed with known contact

The above is not meant to be an exhaustive list of protective measures as each business is unique and may require additional considerations. **You should regularly consult the** FBI **and the** Ic3 website **for updates as well as your legal counsel for additional guidance.**

National Law Review, Volume IX, Number 163

Source URL:https://natlawreview.com/article/reports-hacking-and-wire-fraudbec-scams-increase-here-s-what-you-can-do-to-prepare