COVID-19 Cybercriminals Are Stealing $Billions Using Business Email Compromise (BEC)!

Article By Peter Vogel
Foley & Lardner LLP

Communications, Media & Internet
Coronavirus News
Criminal Law / Business Crimes

All Federal

Tuesday, June 23, 2020

AARP reported that “BEC attacks targeted more than 30,700 organizations in the first quarter of 2020, according to security company Symantec. The FBI says fraudsters are exploiting disruptions in business operations caused by the coronavirus outbreak to perpetrate new variations on the scam, in some cases hijacking Paycheck Protection Program loans to small businesses.” The June 10, 2020 report entitled “Business Email Compromise” included WARNINGS and DO’S AND DON’TS, and as well these comments about the 2 varieties of as “CEO fraud,” “W-2 phishing,” “email account compromise” and “business email spoofing”:

An employee with access to company accounts receives an urgent email request, ostensibly from a top executive, to wire a large sum of money for what sounds like a legitimate purpose, such as an acquisition or vendor payment. The message includes routing data for a bank account that’s actually controlled by the fraudsters, often at a foreign bank. In a variation on this scam, the email supposedly comes from a vendor looking to change its payment account.

The bogus executive emails someone in the payroll or human resources office seeking a list of employees and copies of their W-2 forms. That
potentially puts a wealth of workers’ personal and financial information — Social Security numbers, home addresses, wages and tax withholding — into scammers’ hands, setting the stage for large-scale tax ID fraud and other forms of identity theft.

Please be careful since the Cybercriminals are using Covid-19 to take your money with BEC!

© 2020 Foley & Lardner LLP

National Law Review, Volume X, Number 175