



FEDERAL BUREAU OF INVESTIGATION

Private Sector Advisory

(U) Scam Alert – Spoofed E-mails/Traveling Executives

(U) FBI Dallas is aware of a scam victimizing businesses nationwide using a variation of the scheme detailed in the Private Sector Advisory titled “Nigerian Cyber Criminals Using “Man-in-the-E-mail” Fraud Scheme to Interfere with Business-to-Business Communications,” dated July 5, 2013. The subject, in this new variation, targets an employee authorized to make large wire transfers by impersonating two high-level executives in a spoofed e-mail and requesting the employee to quickly wire a large sum of money for a corporate business deal. The spoofed e-mail address contains a domain similar to the company’s legitimate domain and contains the executives’ correct usernames. Due to the success of the scheme, FBI Dallas is requesting InfraGard Chapter members to report similar incidents to the Internet Crime Complaint Center at www.IC3.gov.

(U) Scheme details:

- (U) The subject identifies the targeted company's e-mail domain and registers a similar domain to create the spoofed e-mail.
- (U) In many cases, the subject identifies when the company executives are traveling. (The subject may have conducted research on social media sites or compromised the executive’s e-mail account.) When the executives are out-of-town, the subject sends an e-mail to an individual in the company responsible for bill pay such as the comptroller. The e-mail usually appears to come from the company’s CFO requesting the wire transfer on behalf of the CEO. To make the request appear legitimate, the e-mail contains a fraudulent e-mail chain started by the CEO requesting the transfer. (It is unknown how the subject knew the comptroller’s legitimate e-mail address but may have located it online or through a computer intrusion.)
- (U) The e-mail consistently asks for money to quickly be wired to a specified account and usually states that the wire transfer should be coded to “Misc. Expense-executive” or “Admin-Expense.”
 - (U) Example of e-mail text: Process a wire of \$84,000 to the attached account information. (The first name of the CEO) will provide me the necessary paperwork later. Code to Misc. Expense – executive. Send me the confirmation when done.

(U) FBI Dallas requests that targeted companies report similar incidents and maintain the e-mails with the original extended headers and any attachments such as .PDF files that provide directions for the money transfers. Thank you in advance for your assistance.