Cyber Fraud in SE Asia

- BEC Frauds
- Inpersonation Scams
- Romance Scams

- 12 Month Statistics
- ~$60M in losses

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise The $26 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses[2]. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.

Who Are the Victims?

- Business of all sizes

- Business that routinely deal in foreign transactions

- Recent victims include universities, multi-national corporations, etc.

How to Protect Yourself

- **Employ two-step verification procedure for wire transfers**
- Employ intrusion detection systems that flag similar email extensions
- Add internal controls to identify and scrutinize changes in vendor payments
- Better scrutiny of email requests for funds transfers

What To Do If Victim of BEC?

1) Contact your financial institution immediately
   - Request your FI contact the recipient FI
2) Contact law enforcement
   - FBI works closely with host nation law enforcement FBI/FinCEN can use rapid response protocol to attempt to reverse wires
3) File a complaint with www.ic3.gov