MS-ISAC

MS-ISAC Security Primer

Business Email Compromise

June 2017, SP2017-1632

State, local, tribal, and territorial (SLTT) governments are frequently targeted by Business Email Compromise (BEC) scams that attempt to deceive SLTT governments into sending money or personally identifiable information (PII), or that use the government's name to fraudulently obtain material goods. The variants targeting SLTT governments include the purchase order fraud variant, W-2 and personally identifiable information (PII) variant, and the financial theft variant. The emails often originate from compromised, spoofed, or fraudulent accounts, which are used to issue a request, and are associated with significant data or financial loss among SLTT governments.

RECOMMENDATIONS: The MS-ISAC recommends that organizations:

- **Craft a policy** for identifying and reporting BEC and similar phishing email scams. Make sure to include the following:
  - When receiving unusual financial or sensitive data requests, users should **verify the identity** and authority of the email sender via standard (non-email) channels.
  - Users should **hover to discover**, to ensure that the email is going to the correct person. The true recipient of an email can often be verified by hovering the mouse over the address in the email header.
  - Users should **reply by forwarding**, and not by hitting the "reply" button, which helps to prevent successful spoofing attacks.
  - Users should **report** suspicious emails to security staff. The MS-ISAC also appreciates receiving notifications of all BEC scam attempts.
- **Train staff** in the finance and human resource departments to identify potential BEC scam emails and follow the suspicious email policy. Indicators of BEC spam emails can include:
  - Poorly crafted emails with spelling and grammar mistakes, that include a note indicating the email was sent from a mobile device (e.g. iPhone, iPad, Android, etc.) in order to convince the recipient the mistakes can be ignored.
  - The wrong or an abbreviated signature line for the supposed sender.
  - The use full names instead of nicknames and a language structure may not match how the supposed sender normally communicates.
  - That the only way to contact the sender is through email. In some cases, the emails appear to be timed to correspond with times the senior official is out of the office.
  - The transactions are for a new vendor or new contract.
  - Internal warning banners that indicate the email is spam, spoofed, or from an external source.
- **Implement filters** at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- **Flag** emails from external sources with a warning banner.
- **Report BEC scams** at https://bec.ic3.gov/. Tax-related suspicious emails should be reported to the IRS at https://www.irs.gov.
- Refer to the MS-ISAC's primer on Spear Phishing, which is available at: https://www.cisecurity.org/white-papers/cis-primer-phishing/.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.