MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
July 2019-SP2019-0860

Business Email Compromise

State, local, tribal, and territorial (SLTT) governments are frequently targeted by Business Email Compromise (BEC) scams that attempt to deceive victims into sending money, personally identifiable information (PII), or material goods, or modifying direct deposit information. The emails often originate from spoofed, compromised, or fraudulent email accounts and if fulfilled may result in significant financial loss or data exposure. Initial emails will likely contain friendly language such as “hi, are you working today?” in order to initiate an email conversation with the victim. The follow-on email will then request the transfer or other action. These emails often use slightly inaccurate terms, such as referring to an employee by a full name instead of a nickname, including a line to indicate they originate from a mobile device in order to excuse mistakes, and including a sense of urgency or secrecy with language such as “ASAP” or "surprise" to make the recipient more likely to quickly comply with the request.

- Direct Deposit Variant: In this variant the scammers pose as the victim and email a direct deposit change request to the finance or human resources department. This results in the employee's paycheck being redirected to an account controlled by the scammer.
- Vendor Account Change Request Variant: This variant is similar to the Direct Deposit Variant, although the request spoofs a vendor and requests the SLTT government modify the vendor’s payment account. The next payment to the vendor is then sent to the updated account number, which belongs to the scammer.
- Vendor Purchase Order Variant: In this scheme, the scammers obtain publicly available purchase order forms and change the contact details on the forms to include different telephone numbers and email addresses. Occasionally, the scammers create copycat websites to authenticate the contact information include on the fraudulent purchase orders. The scammers submit the purchase order to a vendor, have the goods shipped, and sell them for profit while the bill goes to the affected entity.
- Financial Theft Variant: In this variant, the scammers pose as an employee or senior official and request the department immediately wires money for a special purpose. Occasionally, the spoofed email will not directly reference a wire transfer, but rather specified that “transactions” need to be “set up and processed.”
- Gift Card Variant: The scammers perpetrate this variant by posing as a senior official and sending an email requesting the employee purchase gift cards for a surprise award. Once the cards are purchased, the scammer asks for the gift card numbers and pins, claiming they need to immediately give out the awards.
- W-2 and PII Data Theft Variant: In this variant, the scammers pose as an administrator or senior official and send an email to the human resource or finance departments requesting all the employees’ W-2 information or PII. These emails target schools and local governments, with the scammers crafting an email to appear as though it is from a school superintendent or high-level government official. If the employee complies without encrypting the data or encrypts the data and provides the password, this variant results in a data breach. The MS-ISAC believes W-2 information and PII stolen in this manner are often used to commit tax fraud and identity theft.

RECOMMENDATIONS:

- Flag external emails with a warning message in the subject or body. Warning banners can be added by creating Transport Rules on email servers for inbound messages.
- Create a policy for identifying and reporting BEC and similar phishing email scams. Make sure to include the following components:
    - When receiving unusual financial or sensitive data requests, users should verify the identity, authenticity, and authority of the email sender via non-email channels.
    - Users should 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 or double clicking on the name.
    - Users should reply by forwarding, and not by hitting the "reply" button, which helps to prevent successful spoofing attacks.
- Train staff in the human resource and finance 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.
    - The wrong or an abbreviated signature line for the supposed sender.
    - An indication that the email was sent from a mobile device.
    - The use of 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.
    - The transactions are for a new vendor or new contact at a known vendor.
- Ensure human resource and finance department employees have a policy for out-of-band verification (e.g. verbal confirmations, etc.) of requests and an office culture exists in which staff feel comfortable asking if the emailed request is authentic.
- Collaborate with human resource and finance departments to ensure their policies are supported by technological solutions.
- Develop a BEC Incident Response Plan including emergency contacts with the appropriate financial institutions in case it becomes necessary to stop a transfer.
- Implement filters at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- Refer to the MS-ISAC's primer on Spear Phishing for other recommendations.
- Implement the use of Domain Message Reporting & Conformance (DMARC).
- Report BEC scam attempts to the MS-ISAC, local law enforcement, and the Internet Crime Complaint Center (IC3). Tax-related suspicious emails should be reported to the IRS. If there is a financial loss, notify the bank to stop payment and involve local law enforcement.

If financial loss or the transfer of information occurs:

- Immediately contact the financial institution to halt the payment transfer or request assistance in recalling the funds.
- Contact law enforcement and notify them of what occurred. State Police and the Federal Bureau of Investigation (FBI) investigate these crimes.
- During the investigation, ensure the email originates with a spoofed or fraudulent email account and not a compromised account. If an internal email account was compromised, investigate the email server to ensure rules were not created to auto forward emails and to determine the extent of the compromise.

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 is available at 866-787-4722, SOC@cisecurity.org. The MS-ISAC is interested in your comments - an anonymous feedback survey is available.