OHIO AUDITOR OF STATE
KEITH FABER

88 East Broad Street
Columbus, Ohio 43215
ContactUs@ohioauditor.gov
(800) 282-0370

To: All Ohio Auditor of State Clients

From: Keith Faber, Auditor

Date: March 9, 2023

Subject: **PAYMENT Re-Direct and Business Email Compromise Schemes**

Recently, the Auditor of State's Office has observed an increase in Ohio governments falling victim to PAYMENT "Re-Direct" Schemes and business email compromise (BEC) schemes. This is a type of spear phishing attack that has the objective of "re-directing" money to a bad actor, a cybercriminal pretending to be a vendor or employee of the government and then re-directing funds into fraudulent accounts. In these BEC/"re-direct" schemes the cybercriminal impersonates the vendor or employee in an email and requests a change to the bank account. The email impersonation can happen at the start of an email thread or in the middle of a legitimate communication with the cybercriminal compromising an email account or impersonating an email account. When one email account is compromised, within or outside of the local government, all parties on an email thread are also at risk of becoming compromised. Unsuspecting Ohio governments, thinking they are dealing with a known vendor or employee, are processing these requests and changing banking information, without independently verifying the legitimacy of the request or validating the identity of the purported requester.

Government employees should have a heightened sense of scrutiny any time they receive a request to change payment banking information.

While the recent re-direct schemes occurred through electronic communications, it's important to note that these same schemes can be initiated via telephone or physical paper requests as well.

Ways to Identify BEC/Re-direct Schemes

- Pay close attention to the name of the employee or vendor – oftentimes cybercriminals make subtle changes to names to make you think you are communicating with a legitimate or known person/vendor. For example, can you spot the subtle difference between these two emails schoolsolutions@gmail.com vs. schoolsolutiions@gmail.com? The second email address included an extra "I" in the vendor name.

- The email or invoice was unexpected. Unless you are expecting an email, never click on links or open attachments without first verifying the authenticity of the message.

- The email or invoice comes with a sense of urgency including a positive (reward) or negative consequence for not acting quickly.

- Targeted attacks may arrive when they know the CEO or high-ranking official is not available to confirm requests. By following social media posts, the criminals may choose to act when, for example, your executive is on a cruise.

Ways to Stop BEC/Re-direct Schemes

- ***Stop and Think!!!***

  Does the change request make sense? Were any of the red flags above noticed in the request?

- ***VERIFY and VALIDATE***

  NEVER make a change to vendor or employee's contact information or banking information without **independent verification**. **In-person communication** is always the best practice for verifying identity and contact information. Never use email to verify change requests.

  o Require in-person verification for change requests for payment information where possible. It is the best practice to also use a second person verification where the vendor is not personally known by the paying agent, by having the person or department which deals with the vendor personally also verify the identity and confirm the change request.

  o If distance prevents verifying identity and contact information in-person, use only an independently verified contact person and telephone number. Do not use contact information from the change request; instead, find a phone number from a validated source such as a prior invoice or a regularly updated employee or vendor contact information listing. Another source for a valid telephone number is searching for the company's known website.

  o When using a telephone call to validate the identity of an employee or vendor contact, always ask the employee or vendor a question related to past experiences or conversations that only he/she would know the answer to.

  o Require a secondary approval (internally) for all payment requests, payment instruction changes, and changes to employee or vendor contact information. The payment change initiation and payment approval functions should be segregated.

- ***Provide continual training and education*** over policies, procedures, protecting personal information, and recent cyber and phishing threats so that employees can identify fraud schemes before taking compromising actions.

- ***Use added layers of authentication and security*** such as a financial institution's positive pay, ACH positive pay, and ACH Debit Block programs.

Additional Cybersecurity resources, including Incident Response tips and free training, are available on the Auditor of State's website at ohioauditor.gov/fraud/cybersecurity.html.