OHIO AUDITOR OF STATE
KEITH FABER

Auditor of State
Bulletin 2024-003

DATE ISSUED: **April 12, 2024**

TO: **All Public Offices**
All Community Schools
Independent Public Accountants

FROM: **Keith Faber**
Ohio Auditor of State

SUBJECT: **Payment Re-Direct and Business Email Compromise Schemes**

Bulletin Purpose

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 a trusted vendor, business partner or employee in an email and requests a change to the bank account, investment account, or a transfer of funds to a specified bank account unaffiliated with the legitimate business.

Ohio governments are increasingly falling victim to cybercrimes in the form of payment "re-direct" and business email compromise schemes. On March 9, 2023, the Auditor of State (AOS) issued an Advisory, alerting Ohio governments of an increase in cybercrime, providing guidance on what to look for as well as steps to prevent attacks. AOS is issuing this bulletin in response to the continuing reports of cybercrime activity. The following will set clear standards and expectations for Ohio governments and public employees regarding the handling of requests for payment re-directs. **Failure to follow the guidance in this Bulletin may result in an AOS finding when a loss occurs, and the employee is considered liable as a result of negligence or performing duties without reasonable care.**

Typically, these payment re-direct and business email compromise schemes are tailored to specific entities or individuals and are commonly referred to as a spear phishing attack. The cybercriminal's goal is to deceive the entity or individual into sending funds or payments to compromised or false bank accounts – often by posing as a trusted vendor, financial institution, or another member of the compromised organization. The cybercriminal will closely mimic actual emails, invoices, vendor documents, bank accounts or other electronic communications to lead the entity or individual into believing the request to re-direct funds or deposits is legitimate.

Often, in these cases, cybercriminals will breach an entity's information technology system through compromised email, attachments and malware only to then hide and wait for an opportunity to exploit. The email impersonation can happen at the start of an email thread or in the middle of a legitimate communication, with the cybercriminal compromising or impersonating an email account. When one email account is compromised, within or outside of the government, all parties on an email thread are at risk of becoming compromised. Unsuspecting Ohio governments, thinking they are dealing with a known vendor, financial institution or employee, process the payment re-direct or change banking information, without first independently verifying the legitimacy of the request and validating the identity of the purported requester. These schemes also include requests from employees to update or change their bank routing information for payroll and other employee directed withholdings.

While many re-direct schemes occur through electronic communication (e.g., email), it is important to note that these same schemes can be initiated via telephone or physical paper requests as well. With advancing artificial intelligence technology, these cybercriminals can match voices and appearances electronically.

The increasing frequency of successful attacks have resulted in significant financial losses for governments. Accordingly, all government employees shall adopt a heightened sense of scrutiny any time they receive a request to change payment, investment or banking information. In addition, governments need to proactively train their employees and create an organization-wide culture of security to prevent fraud. Finance teams and/or employees processing invoices are the most vulnerable to this type of fraud as they often receive payment and re-direct requests. However, all employees should be aware of these fraud schemes as anyone can fall prey to a spear phishing attack that could open the organization up to further exploitation.

Real Examples of Fraud or Potential Fraud

- **Spear phishing**: More than $700,000 was stolen from a recreation district because of a payment re-direct scheme. Emails were received by the district, from an email account slightly different than the original vendor email account, which contained erroneous payment instructions to the "vendor." The district followed the instructions and transferred $713,094 to the fraudulent account, without independently verifying the identity of the requester or the new banking account.

- **Spear phishing:** A city fell victim to a "spear phishing" scheme resulting in theft of nearly $219,000 when the finance department received emails from someone pretending to be an existing vendor. The email persuaded the employee to change the bank account routing information the city had for the vendor. Vendor verification protocols were not followed, which could have prevented this fraud.

- **Investment account change request:** A college fell victim to a spear phishing attack that included convincing branding and logos of a financial institution causing the college to change account information on a $6 million account. Realizing a day later due to *Daily Cash Monitoring* protection that the money was not in its account the college was able to recover the funds through the activation of the Financial Fraud Kill Chain.

- **Fraudulent check and Electronic Funds Transfer/ACH scheme:** A city reported three instances of fraudulent checks submitted for payment to their bank and two instances of attempted ACH fraud. Though none of these instances were successful and the city did not experience a loss, this is another example of attempted fraud.

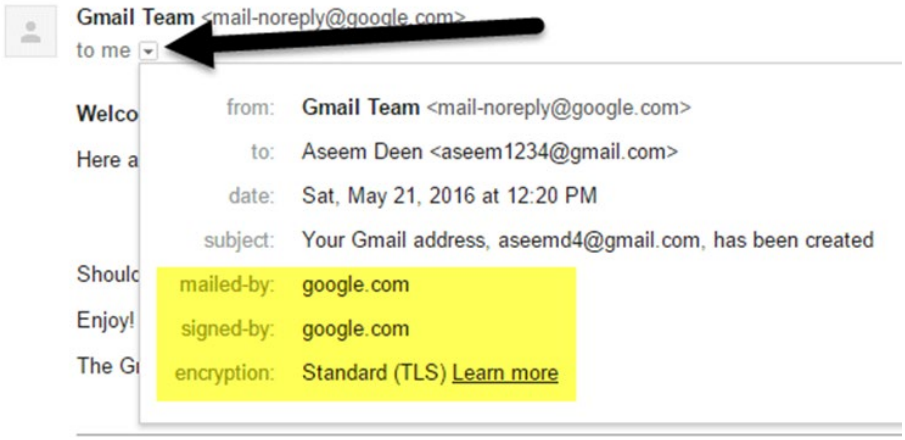
Ways to Identify Re-direct and Business Email Compromise Schemes

- Pay close attention to the name of the employee or vendor — cybercriminals often will 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 email addresses schoolsolutions@gmail.com vs schoolsolutiions@gmail.com? The second email address, the fraudulent one, includes an extra "i" in the vendor's name. Considering the search capabilities of the internet, cybercriminals often have full staff directories of vendors and government offices to determine who to mimic and who to target.

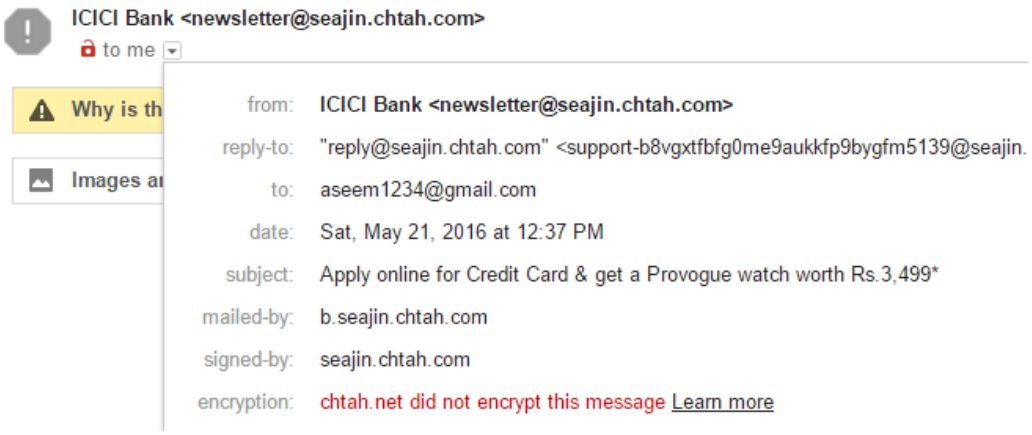
- An email or invoice that is unexpected is received. Unless you are expecting an email, never click on links or open attachments without verifying the authenticity of the sender and the message or attachment.

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

- Carefully review the email sender's details. Hover your cursor over the sender's email and a window will pop up. In the example, below, we clicked on the arrow underneath the sender's gmail name. The most important items to look at are the "mailed by," "signed by," and "encryption" fields. Here, the message was mailed by and signed by google.com and was encrypted—all signs that the email is genuine.



- Below is an example of a fake email purporting to be from a bank. The clues: The email address doesn't sound like a bank; the "mailed by" and "signed by" fields are the same as the suspicious name; and the email was not encrypted. All signs the email is probably fake.



- The email contains obvious misspellings or strange diction and grammar.

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

Ways to Prevent Re-direct/BEC/ACH Schemes

- **Stop and consider for a moment:** 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, financial institution or employee's contact information or banking information without independent verification. Avoid taking re-direct requests by electronic means. In-person communication is always the best practice

for verifying identity and contact information. Never use email or embedded phone numbers to verify change requests.

- Always require in-person verification of employee payroll re-directs. Never take such requests electronically.

- Request in-person verification for change requests for payment information. Have the vendor come to the office in-person to provide re-direct payment information. Where the vendor is not personally known to the paying agent, you should have a second person from the department that deals with the vendor personally verify the identity, confirming the change request.

- If circumstances prevent verifying identity and contact information in-person, use extreme caution and only an independently verified contact person and telephone number, via separate sources. 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 the company's known website.

- 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. Offering to contact the requester back will allow you to validate the number to ensure it is linked to the vendor.

- Require an internal, secondary approval 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.

- Consider making a partial payment (very small dollar amount) of the invoice or wages to allow for verification from the receiving financial institution, vendor, or employee as to the legitimacy of the payment.

- **Provide continual training and education** over policies, procedures, recent cyber and phishing threats, and how to protect personal information so that employees can identify fraud schemes before taking compromising actions. Contract with a vendor or use association services for employee cyber training and insurance coverage.

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

- **Create security policies** that outline best practices for protecting sensitive data and systems. The policies should include information related to password management, data encryption, software updates and other security measures that employees should follow.

Guidance

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.

Resources for reporting fraud can be found at ohioauditor.gov/fraud/default.html.

Questions

If you have any questions regarding the information presented in this Bulletin, please contact the Special Investigations Unit at the Auditor of State's Office at PaymentSchemeQuestions@ohioauditor.gov.

Keith Faber
Ohio Auditor of State