Emerging Issues Task Force Hot Topic

Hot Topic Number: 17-01

Date Posted: June 28, 2017

Hot Topic Heading: Wire Transfer Fraud

Description

Municipal administration should be aware of various ***business e-mail scams*** that are happening all around us. Many of these scams involve wire transfer fraud and are done through "executive impersonation" where an imposter pretends to be a senior executive requesting a payment for an urgent business transaction. Adequate internal controls and awareness can go a long way to prevent fraudulent requests from proceeding and the imposter from profiting. Below is some helpful information to protect your municipality from falling victim to such a scam.

Things you need to know about common fraud schemes

- Often times the imposter will research the municipality through social media such as Facebook and Twitter. In doing so, information will be obtained about the senior executives such as the Mayor or City Manager which make it easier for them to pretend that's who they are.
- The scheme often begins with an employee receiving e-mail from the imposter who mimics the senior executive with a request for a payment, which usually has some urgency to it.
- The e-mail will often be sent while the senior executive is out of town, for example, during the AUMA or AAMD&C conferences. This sets up the premise that communications must be done through e-mails, which make the act of impersonation easier for the scammer.
- The e-mail correspondence may not look suspicious at first glance because the imposter has completed research to mimic the format of standard emails. Even the writing style may look appropriate and the "from" e-mail address may appear to be correct.
- The imposter may provide an invoice for the requested payment or transfer that will include the banking information that the employee would need in order to complete the transfer. The requested transfer will often be made to a foreign bank and there would likely be limited details about the project that the funds have been requested for.

- Although approximately 56% of the time the requested payment form will be wire transfer, other forms of payment such as checks, corporate/commercial credit cards, automated clearing house (ACH) debit or ACH credits may also be requested.

Ways to mitigate your risks

- Maintain an adequate system of internal controls, which include standard operating procedures and authorization processes for paying invoices or requisitions.
- Provide training to financial staff, audit committees and senior officials in regards to wire transfer fraud.
- Be suspicious of any unusual payment requests. Although the initial e-mail may look authentic, there may be subtle spelling/grammar mistakes or inconsistencies that can expose the scam, especially in follow up e-mails.
- Whenever possible, confirm all payment requests that are not done through standard practices by contacting the requestor directly through telephone or interoffice communication media.
- If you are suspicious, have an IT professional investigate where the email originated by tracing the IP address.

Sources:

City of Lethbridge – Alberta City Treasurers' Meeting presentation, November 4, 2016

Ernst & Young – Preparing your organization for Wire Transfer Fraud, Infonex – Internal control training, October 28, 2015

Association for Financial Professionals, 2016 AFP Payment Fraud and Control Report: HTTP://https://www.pnc.com/content/dam/pnc-com/pdf/corporateandinstitutional/Treasury Management/2016_AFP_Fraud_Report.pdf

Author: Hot Topics Initiative Subcommittee