OIG In Your Inbox

Insights, Advisories and Alerts

Vol. 1, Issue 2 | July 2025

Detect and Prevent Electronic Funds Transfer (EFT) Fraud

Municipalities face a growing variety of cybersecurity risks, including data breaches, ransomware attacks, and denial of service (DoS) attacks. These risks can result in a variety of harms to the municipality, including loss of access to critical infrastructure, disclosure of confidential information, and reputational damage. Cybersecurity risks can also result in direct financial losses to the municipality through fraudulent payments. One such risk that has affected many Massachusetts communities is the use of phishing tactics to conduct Electronic Fund Transfer (EFT) fraud.

Identifying the Threat

Phishing is a cybersecurity attack that relies on social engineering as much as technical expertise. A phishing attack sends communications, such as emails, that appear to come from an individual whom the target would likely trust, such as a coworker, client, or authority figure. By tricking the target into believing the communication comes from a trusted source, the attacker can cause the target to let down their guard when engaging with the message. A classic example of a phishing attack is an innocuous-seeming email containing a link or attachment that, when opened, installs malware on the target's computer.

EFT fraud is a form of fraud in which the attacker learns about an anticipated payment for services rendered, such as from a vendor or contractor, and fraudulently causes the EFT to be sent to a bank account controlled by the attacker or their associates. Once the EFT is made, the attacker quickly removes the stolen funds from the bank account before the EFT can be reversed.

Attackers can use phishing tactics to conduct EFT fraud by sending a phishing email, or series of phishing emails, to gain the trust of the targeted individual, who is typically someone responsible for receiving invoices or processing EFT payments on behalf of an organization. The goal of the phishing attack is to trick the target into sending an EFT payment to the bank account controlled by the attacker. This is typically done by providing new or substitute wiring instructions by email, or by changing the wiring instructions on an emailed invoice.

Municipalities are as vulnerable to EFT fraud through phishing tactics as any business. Municipalities often engage with outside vendors and contractors for procurement of a variety of services. And they typically

pay vendors and contractors via EFT payments processed by the financial officer or treasurer, or their staff. While this is a better practice than allowing multiple employees to make decentralized payments through multiple credit cards, challenges persist that put municipalities at risk. No matter the size, municipalities face issues from staff turnover to staff size to staff training. All of this leaves a municipality vulnerable to EFT fraud, particularly if the attacker can successfully phish an individual responsible for processing payments.

Adopt a mandatory policy that employees must verbally verify EFT bank information when they receive new wiring instructions or requests to update or change banking information. Require employees to call the requestor on a phone number obtained independently from the email containing the new wire instructions or the invoice containing new bank information.

The damage caused by EFT fraud can be large: EFT scams carried out through phishing tactics have defrauded Massachusetts municipalities of millions of dollars.

What You Can Do

There are several steps that you can take to detect and prevent EFT fraud in your municipality:

1. Train individuals responsible for making EFT payments to verify changes to bank information through a method other than the one the sender used to submit the request. For example, if a vendor sends you an email with updated wiring instructions, call the phone number listed on the vendor's official or verified website, rather than the phone number listed on the wiring instructions, to verify the request and the new bank information.

2. Divide accounting duties among multiple employees and implement a system of approvals concerning changes to bank information. Any request to change established payment methods, amend payment schedules, or create a new payment method should trigger verification procedures.

3. Reconcile municipal account statements with vendor invoices and bank statements on a timely basis to promptly identify improper payments and increase your chances of recovering stolen funds.

4. Implement mandatory cybersecurity training for municipal employees during their onboarding and at least annually thereafter. Organizations like the Cybersecurity and Infrastructure Security Agency (CISA) offer free resources that organizations can use to kickstart efforts to educate their staff on current threats.

5. Confirm that your cybersecurity training contains instructions and tips for recognizing signs of a phishing attack, such as:

    - Instructions containing a sense of urgency;

    - Instructions purportedly from a CEO to immediately act, though the CEO is unavailable to discuss the request;

- Requests for personal information;
- Poor grammar and spelling; or
- Unusual senders or apparent impersonation.

6. Ensure that individuals responsible for receiving invoices and making EFT payments receive up-to-date cybersecurity training.
7. Encourage municipal employees to be on alert for phishing communications, including from internal sources.
8. Make sure that your email system has a method for reporting suspicious communications and that your IT officer has a process for reviewing those reported communications.
9. Encourage municipal employees to maintain good security hygiene, such as regularly changing passwords and adding Multi-Factor Authentication (MFA) to security systems.

Conclusion

Cybersecurity risks are continually evolving. Responding to them requires constant vigilance and regular evaluation of organizational defenses. Maintaining a robust culture of cybersecurity training and awareness is one of the best defenses against these evolving risks, particularly when confronting social engineering tactics such as phishing.

*The OIG periodically issues **OIG In Your Inbox: Insights, Advisories and Alerts** as a way to succinctly share timely topics with key stakeholders, most notably the leaders within the Commonwealth's 351 local communities. The OIG hopes that **OIG In Your Inbox: Insights, Advisories and Alerts** will prompt dialogue and needed action on matters important to public entities.*