Finance Professional’s Cheat Sheet for Fighting Cybercrime

A cyber scam known as fraudulent instruction/transaction is responsible for some of the largest thefts involving Texas school districts. In one attack, **a district lost more than $2 million**. These scams typically hinge on business managers, payroll clerks, accounts payable, and other employees who have access to district finances taking the bait. Follow these tips to protect yourself and your employer.

Learn the most common scams
The cybercriminals behind fraudulent instruction/transaction attacks fabricate emails that appear to come from vendors or district employees. The emails ask you to send payment for services to an account the criminal controls. Here are three seemingly legitimate requests you might receive:

- A fake construction company representative insists that you send an overdue payment or change their bank account information in your records.
- An email that appears to come from the superintendent or another district leader asks you to send payment to a vendor.
- A district employee asks you to change their direct-deposit account information.

Review email subject lines
Check for words common in fraudulent email subject lines, such as urgent, request, payment, transfer, invoice due, and direct deposit.

Scrutinize the sender’s email address
Hover over names in the “From” field and check for misspellings and inaccurate domains. For example, a spoofed email from TASB might come from name@tsba.com instead of name@tasb.org.

Don’t trust links, attachments, or logos
If you suspect an email is fraudulent, do not click on links or open attachments, which can contain malware. Instead, use your browser to search for the company’s official website or phone number. Also remember that company logos, like website and email addresses, can be spoofed.

Implement a dual authentication policy
Fund members with Privacy and Information Security coverage are required to implement a dual authentication policy. Your policy should require employees to consult a pre-designated contact who works for the vendor and verify that requested changes to financial transactions or bank account information are legitimate. Similarly, district employees should be consulted before requests to change their direct-deposit account information are fulfilled.

Avoid wire transfers when possible
Use paper checks instead. If a wire transfer is necessary, ask a supervisor to review and confirm the request before transferring the funds.

TASB™ RISK FUND

Implement controls with financial institutions

Have your finance department director or your chief financial officer work with your financial institution to establish protocols and policies that require secondary authorization for certain large transactions.

Stay alert to vishing scams

Vishing is a fraudulent instruction/transaction scam in which criminals call or send text messages instead of emails. They might even spoof a legitimate phone number:

- **Hang up and call back.** If you receive an unsolicited call requesting sensitive information or encouraging you to take action, end the conversation, investigate the request, and call back later.
- **Question motives.** Think about the caller's motives, especially unanticipated or unidentified callers. Why do they need the information they are asking for? Why do they not already have it?

Report your suspicions

The sooner you contact your information technology department, the sooner they can protect the organization against the scam.

Policy in action

Here are some examples of what these crime-fighting practices look like in action:

- One Texas school district's new procedures require employees to hand-deliver direct deposit change requests to the payroll coordinator. If the office is closed, employees may email the forms to payroll. However, payroll will follow up by calling the personal phone number listed in the employee's HR records and verifying change requests.
- Another district requires that when a direct deposit change request comes in via email, payroll composes a new email (rather than replying to the one that came in) and sends it to the address on file with HR. The email informs the employee about the request and asks them to log into the employee access portal and manually confirm that it's legitimate. The email contains no banking information or account login information, so only the employee should be able to access the portal.

Security vs. convenience

Implementing these cybersecurity measures will create some inefficiencies in payroll and administrative operations. It's also important to remember that a quick direct deposit change can be imperative for an employee's financial well-being. Still, the significant uptick in direct deposit scams requires additional safety measures that protect district funds and employee salaries.