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

Fraudulent instruction/transaction is one of the most damaging modes of attack over the last two years. The cybercriminals behind these 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.

TASB Risk Management Fund cybersecurity experts constantly monitor fraudulent instruction/transaction scams and other emerging threats that target educational entities. Visit our blog regularly at tasbrmf.org/InsideRM to keep up with the rapidly evolving cybersecurity threat landscape.

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.

Confirm transaction requests over the phone

Call – do not email - a pre-designated contact who works for the vendor, and verify that requests to send overdue payments or change bank account information are legitimate. Follow the same process for employee requests to change direct-deposit account information.

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.

Implement controls with financial institutions

Have the director of your finance department or your chief financial officer establish protocols and policies with a representative of your financial institution to 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

If you believe you may be the victim of a cybercriminal attack, immediately report your suspicions to your information technology department, local and federal law enforcement, and your claim representative if you have cybersecurity coverage. Prompt notification enables mitigation personnel to block malicious websites, alert staff, contact appropriate regulatory agencies, and potentially quarantine compromised network segments. The sooner you reach out for help, the sooner your network can be opera