Mineral

Crown Risk Management, LLC

Question of the Week

OCTOBER 12, 2022

QUESTION

We've received suspicious emails that appear to be from employees asking to change their direct deposit information. What should we do?

ANSWER

This is likely a phishing scam—a type of con in which scammers use emails, texts, or phone calls to trick someone into providing company or personal information that then allows the scammer to steal from them. These messages often appear to come from someone the recipient knows—in this instance, your employees.

A successful scam can be a costly data breach with legal consequences for employers. In this case, had you fallen for the direct deposit scam, your employees would not have been paid on time, and you'd be out the money you owed them.

To protect your organization from this and other phishing attempts, we recommend taking the following steps:

- Verify that the message is not legitimate. In this case, inspect the email addresses for validity and reach out to the employees to confirm they didn't request to have their bank information changed.
- Notify your IT department of the potential phishing attempt.
- Inform your workforce that scammers are afoot and remind them not to respond to emails that are suspicious or to email sensitive information. Email is like a postcard, potentially visible

to anyone, so employees shouldn't email their banking or other sensitive information.
- Work with your IT department to train employees how to recognize phishing attempts and what to do if they notice or fall prey to one.
- Ensure employees update their security software, internet browser, and operating system regularly.
- Create processes and policies that staff should follow in case of a breach, including what notices need to be given.

This Q&A does not constitute legal advice and does not address state or local law.