Protect Our Paychecks—Beware of Payroll Diversion Scams

Danger

Criminals are trying to steal employee paychecks through a scam known as "payroll diversion." And they're looking for your help. Don't fall for it.

How payroll diversion works

The criminals' goal is to change employee direct deposit information. If they succeed, the employee's paycheck will be deposited into an account that the criminals control. Once that happens, the money is quickly transferred out of the account.

Because of your role, you may be a target for criminals trying the scam.

Tips to protect yourself

- Be on the alert when you get any request for help with direct deposit, even if it's just a question about how to do it.
- If you receive an actual update to direct deposit instructions, call the employee at a known phone number to confirm they intend to change their direct deposit.
- **Don't** trust any contact information in the request itself. Call using a phone number you know is accurate.
- Know our procedures for handling legitimate requests to update direct deposit instructions.

How to spot a payroll diversion incident

- An employee reports they didn't receive their paycheck.
- An employee reports that they received a paper check instead of the usual direct deposit.
- An employee notices unexpected forwarding or deletion rules in their email account.
- An employee notices email from our payroll provider in their recycling folder.
- You receive an email requesting a change to direct deposit or instructions on how to do so, but after putting your cursor over the employee's email, you notice the email address is different.

What you should do if you get a suspicious email

If you suspect that an email is a payroll diversion email:

- Do not open any links or attachments in the email.
- Notify our IT department.
- **If you've already opened a link or attachment, disconnect your computer from the internet but do not turn it off, and then immediately call IT.**

beazley