1 ADP Boulevard
Roseland, N.J. 07068

Date: October 22, 2021
From: ADP Global Security Organization
Subject: Payroll Diversion Scam: Fraudulent Employee Direct Deposit Information

---

ADP has been made aware of recent fraudulent activity impacting some clients and Payroll / Human Resources (HR) practitioners regarding payroll diversion scams that involve fraudulent direct deposit information.

How Does It Happen?
Cyber criminals attempt to commit payroll fraud by sending fake phishing emails or calling HR and Payroll practitioners requesting a change to employee bank account information. The emails are sent with a request for a change of banking details and appear to use the employee's correct sender name and email signature. Callers have enough information about the real employee to successfully impersonate them. Once the change is made, the employee's payroll is diverted to a fraudulent account.

Common email subject lines for this scam include:
- "Payroll"
- "Urgent Payroll Request"
- "Urgent Request!!"
- "Re: (Employee Name)"

How to Protect Yourself
It is critical that you and your employees be proactive and alert when communicating through email. Be sure the email address is that of your employee and not spoofed. By educating your employees on safe email practices, including how to recognize and report suspicious emails, you can help mitigate the threat of payroll fraud.

- Be cautious of requests for bank account changes that originate via email, especially if the email has a vague or urgent subject line.
- Validate bank account changes directly with your employee before entering them. It is critical that validation occurs through a method other than email (i.e. in person, by calling the known contact number, instant message, etc.).
- If you receive a suspicious email, do not click on any links or open any attachments within the message. Do not reply to the email and immediately contact your IT team to report the email.
- If you receive a phone call asking for a bank account change, do not give out any information or process any changes until you validate the caller's identity through another method (i.e. in person, by calling the known contact number, instant message, etc,).
- If you are an employee and you received a notification of a change that you did not authorize, contact your payroll department immediately.

The ADP Global Security Organization continues to actively monitor this situation. Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.