1 ADP Boulevard
Roseland, N.J. 07068

Date: June 11, 2019
From: ADP Global Security Organization
Subject: Industry Alert – Payroll Fraud - Cybercriminals Targeting HR and Payroll Practitioners

---

ADP is alerting its clients and Payroll / Human Resources (HR) practitioners of an uptick in phishing emails targeting them that involves fraudulent payroll direct deposit information.

**How Does It Happen?**
Cyber criminals try to commit payroll fraud and steal funds by sending fake phishing emails to HR and Payroll Staff requesting a change to 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. 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. 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. phone, in person, instant message, etc.) as the employee's email may be compromised.
- 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 are an employee and you received a notification of a change that you did not authorize, contact your payroll department immediately.

For more information please visit www.adp.com/trust for the latest security alerts, phishing information, security resources and best practices. Protecting ADP clients and their data from malicious activity has been, and always will be, a top priority for ADP.