1 ADP Boulevard
Roseland, N.J. 07068

Date: June 19, 2020
From: ADP Global Security Organization
Subject: Phishing Campaign: "I recommend You review and follow the recommendations in the attachment"

ADP has received reports about fraudulent emails sent to ADP clients. These emails **do not originate from ADP** and our analysis has revealed that they may contain malicious content. We're working with our fraud prevention team and anti-phishing vendor to address this incident.

Message Sender :
"Ozzie<AT>allweekplumbing[.]com" or
"Tmelara<AT>selectmailingequipment[.]com" or
"srs0=xflipq=76=simplygreeninc[.]net=scott<AT>eigbox[.]net" or
"June<AT>ecchvac[.]com" or
"Lsims<AT>beautifulrestaurant-atlanta[.]com" or
"Nebyat<AT>bnaturalcafe[.]com" or
"elmehdi.chafqane<AT>reedmotorsinc[.]com" or
"Rnagle<AT>rknmechanical[.]com" or
"Nebyat<AT>expresparking[.]com" or
"Service<AT>dunwellplumbing[.]com" or
"Avi<AT>probody-shop[.]com" or
"John<AT>pueblofruits[.]com" or
"parts<AT>reedmotorsinc[.]com"

Message Subject :
"I recommend You review and follow the recommendations in the attachment"

How to Report a Phishing Email
Be alert for this fraudulent email. Follow the instructions below if you receive this, or any other suspicious email.

- Do not click on any links or open any attachments within the message.
- Forward the email as an attachment to abuse@adp.com, then delete it.
- If you clicked any link or opened an attachment in the email, immediately contact your IT support.

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.