Date:        July 14, 2020
From:        ADP Global Security Organization
Subject:     Phishing Campaign: "DON'T GET LOCKED OUT"

ADP has received reports about fraudulent emails being 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:
Varying including :
bflowers<AT>olympic[.]edu
irene[.]clark<AT>csun[.]edu
05127<AT>ahu[.]edu[.]
huangyi<AT>cdu[.]edu[.]

Message Subject:
**DON'T GET LOCKED OUT**

**How to Report a Phishing Email**
Be alert for this fraudulent email and follow the instructions below if you receive any 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.

Sign up to have new alert notifications delivered to you by email – visit the alerts section of www.adp.com/Trust for more information.