1 ADP Boulevard
Roseland, N.J. 07068

Date: July 4th, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: “Your email have changed”//“Your security preference has been reset”//“Confirm your email address”

ADP has received reports regarding fraudulent emails being sent to ADP clients that have the following subjects: “Your email have changed, “Your security preference has been reset” or “Confirm your email address”. Please note that we reported a similar phishing campaign on June 6th - the sender address varies but is consistently XXX@tnoculoplastics.com. All emails include links posing as ADP login pages.

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.

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 spam2@adp.com.
- Delete the original email once you’ve received confirmation of receipt from spam2@adp.com.
- If you clicked any link or opened an attachment in the email, immediately contact your local IT support team for further action.
- If you receive external inquiries regarding this email, please advise the email is fraudulent and should be deleted. If the recipient opened an attachment or link, they should contact their IT support.

Security Resources

- Subscribe to Security Wire on ADPworks for security updates and alerts.
- Visit the GSO Services Portal for security contacts, materials, policies, and more.