Date: July 19, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: “Please provide an alternative.” // “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: “Please provide an alternative.” // “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 and July 4th - 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. Please see the example below which may vary in content and sender.
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](http://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.