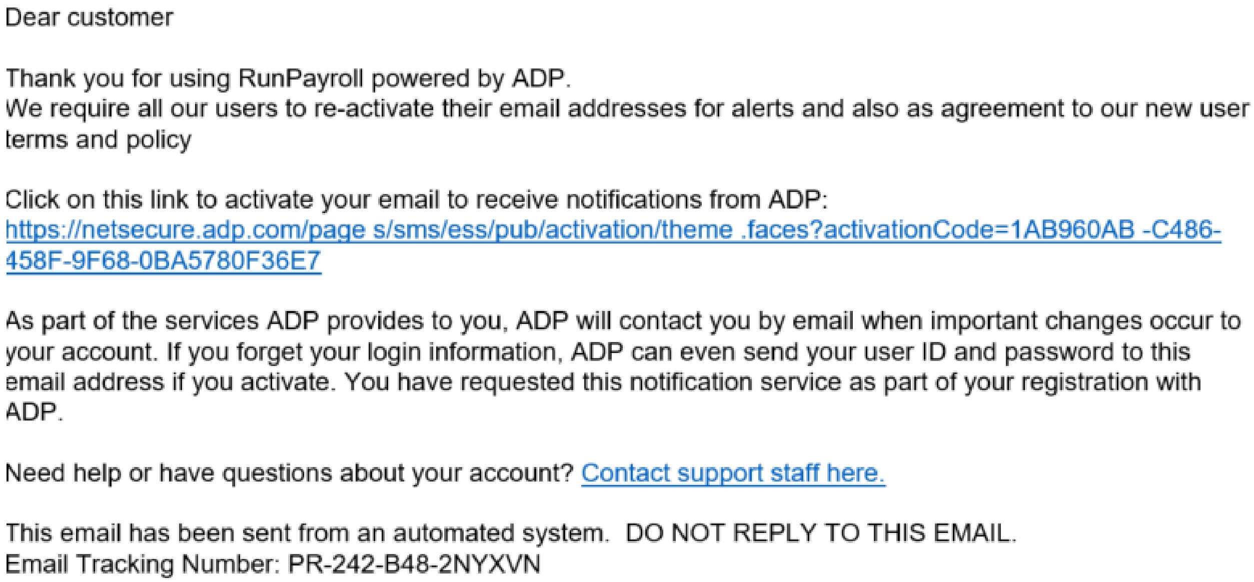
1 ADP Boulevard
Roseland, N.J. 07068

Date: April 3, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: “ADP service center”

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format Nagpal-Shah, Vandana <vnagpal-shah@FanshaweC.ca> with the subject line “**ADP cervice center**”. These emails instruct the recipient to login to Netsecure to re-activate their email address and agree to new terms and policies. Included is a netsecure link that redirects the user to a phishing page.

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 examples below which may vary in content and sender.



Dear customer

Thank you for using RunPayroll powered by ADP.
We require all our users to re-activate their email addresses for alerts and also as agreement to our new user terms and policy

Click on this link to activate your email to receive notifications from ADP:
https://netsecure.adp.com/page s/sms/ess/pub/activation/theme .faces?activationCode=1AB960AB -C486-458F-9F68-0BA5780F36E7

As part of the services ADP provides to you, ADP will contact you by email when important changes occur to your account. If you forget your login information, ADP can even send your user ID and password to this email address if you activate. You have requested this notification service as part of your registration with ADP.

Need help or have questions about your account? Contact support staff here.

This email has been sent from an automated system. DO NOT REPLY TO THIS EMAIL.
Email Tracking Number: PR-242-B48-2NYXVN

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.