1 ADP Boulevard
Roseland, N.J. 07068

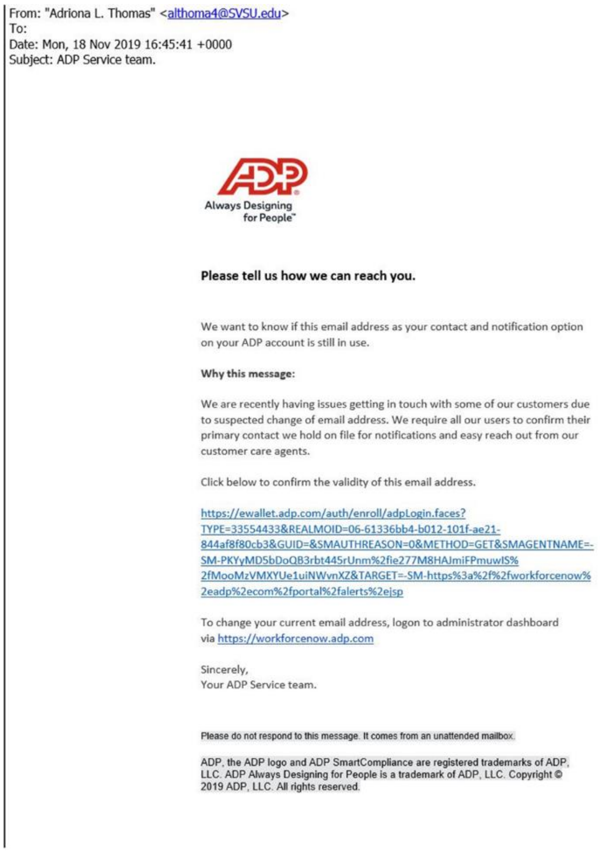
Date: November 19, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP Service team." // "ADP SUPPORT"

ADP has received reports regarding fraudulent emails being sent to ADP clients with the following subject lines: "**ADP Service team.**" and "**ADP SUPPORT**" These emails instruct the recipient to confirm validity of their email address. The link takes the user to a cloned ADP login page.

Message Sender:
Adriona L. Thomas <althoma4><AT>SVSU[.]edu>
Alexandrya L. Weiss <alweiss1><AT>SVSU[.]edu>

Message Subject:
ADP Service team.
ADP SUPPORT

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.



From: "Adriona L. Thomas" <althoma4@SVSU.edu>
To:
Date: Mon, 18 Nov 2019 16:45:41 +0000
Subject: ADP Service team.

Please tell us how we can reach you.

We want to know if this email address as your contact and notification option on your ADP account is still in use.

Why this message:

We are recently having issues getting in touch with some of our customers due to suspected change of email address. We require all our users to confirm their primary contact we hold on file for notifications and easy reach out from our customer care agents.

Click below to confirm the validity of this email address.

https://ewallet.adp.com/auth/enroll/adpLogin.faces?TYPE=33554433&REALMOID=06-61336bb4-b012-101f-ae21-844af8f80cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=-SM-PKYyMD5bDoQB3rbt445rUnm%2fie277M8HAJmiFPmuwIS%2fMooMzVMXYUe1uiNWvnXZ&TARGET=-SM-https%3a%2f%2fworkforcenow%2eadp%2ecom%2fportal%2falerts%2ejsp

To change your current email address, logon to administrator dashboard via https://workforcenow.adp.com

Sincerely,
Your ADP Service team.

Please do not respond to this message. It comes from an unattended mailbox.

ADP, the ADP logo and ADP SmartCompliance are registered trademarks of ADP, LLC. ADP Always Designing for People is a trademark of ADP, LLC. Copyright © 2019 ADP, LLC. All rights reserved.

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.