

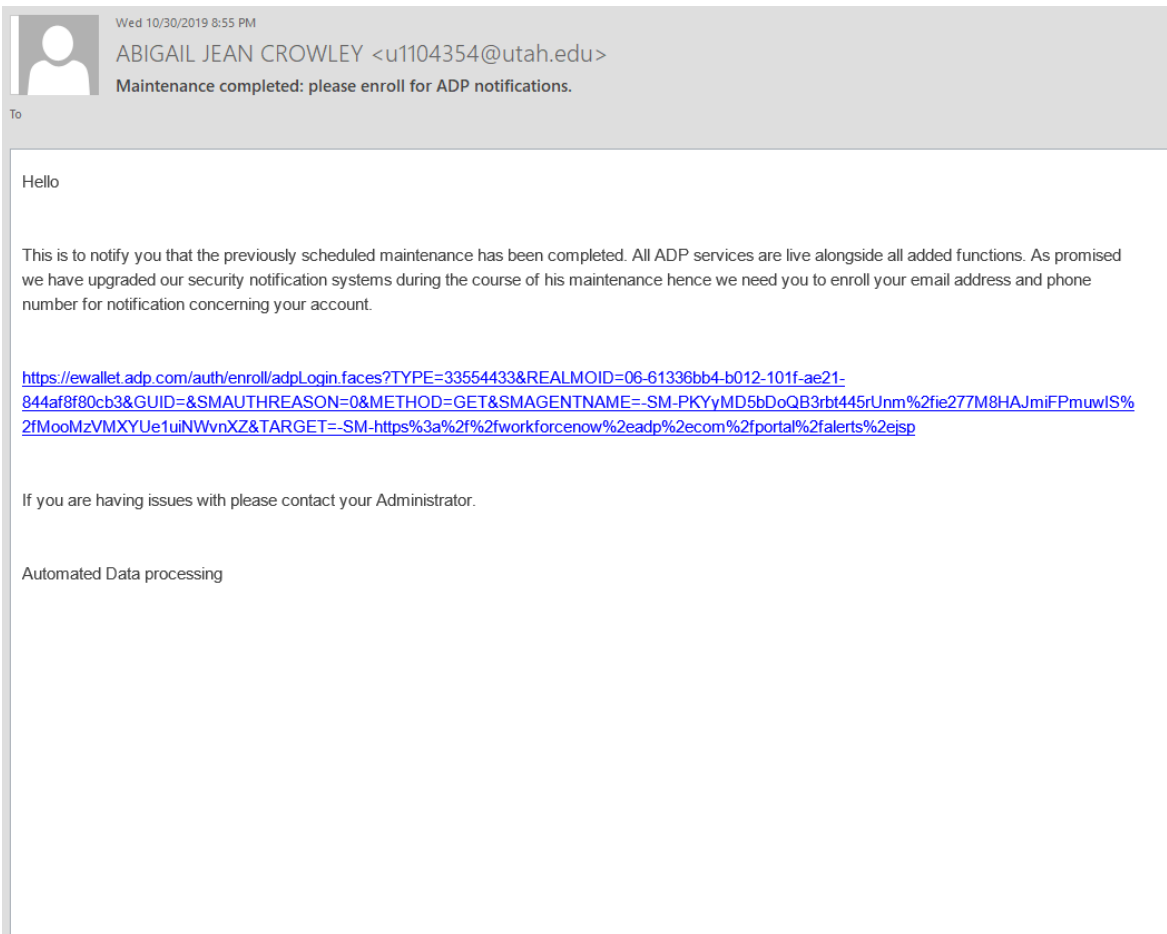
Date: October 31, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP support We've got you covered." // "Maintenance completed: please enroll for ADP notifications."

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: <Display Name><AT>utah[.]edu> with the following subject lines: "ADP support We've got you covered." or "Maintenance completed: please enroll for ADP notifications." These emails instruct the recipient proceed to sign in to their account. The link takes the user to a **WorkForceNow** cloned login page.

Message Sender:
<Display Name><AT>utah[.]edu>

Message Subject:
"ADP support We've got you covered"
"Maintenance completed: please enroll for ADP notifications"

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.



Wed 10/30/2019 8:55 PM

ABIGAIL JEAN CROWLEY <u1104354@utah.edu>
Maintenance completed: please enroll for ADP notifications.

To

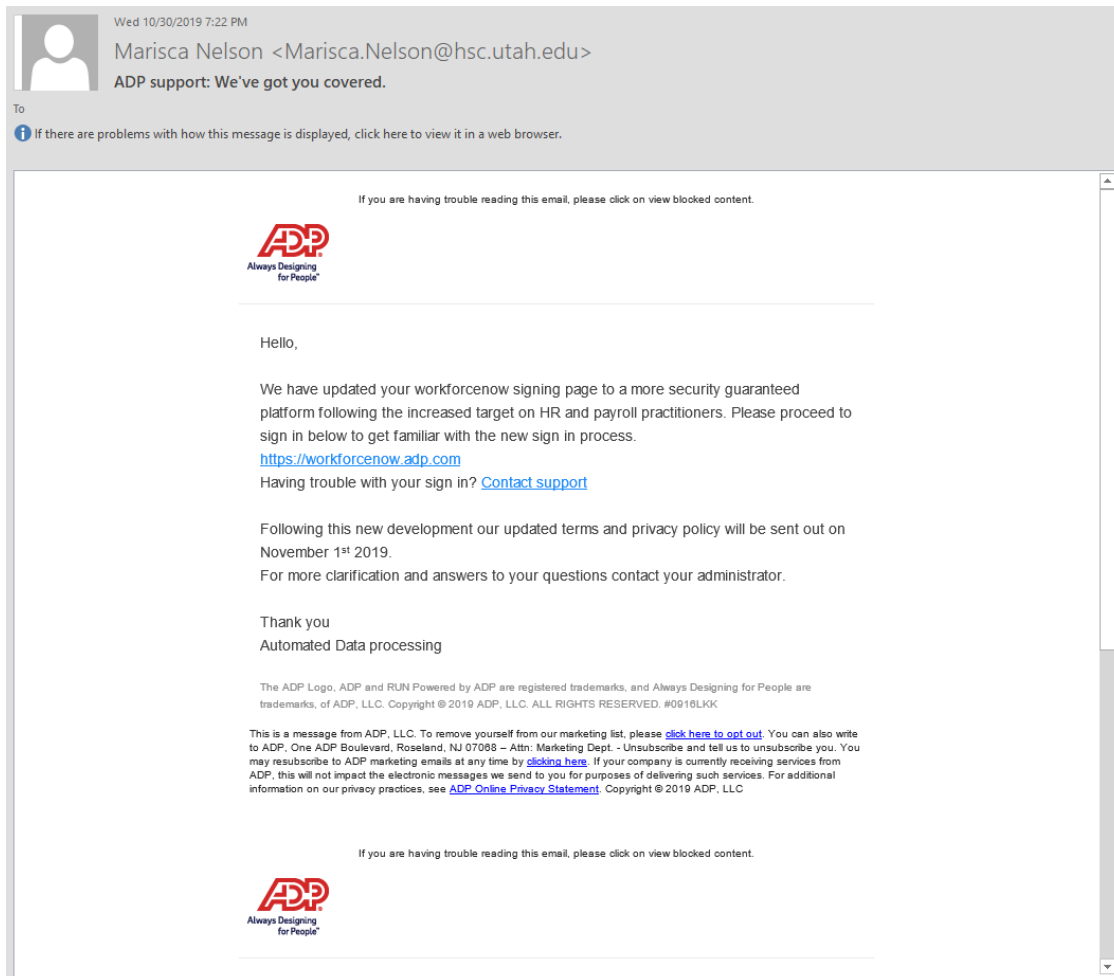
Hello

This is to notify you that the previously scheduled maintenance has been completed. All ADP services are live alongside all added functions. As promised we have upgraded our security notification systems during the course of his maintenance hence we need you to enroll your email address and phone number for notification concerning your account.

<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%2fMooMzVMXYUe1tuiNWvXZ&TARGET=-SM-https%3a%2f%2fworkforcenow%2eadp%2ecom%2fportal%2falerts%2ejsp>

If you are having issues with please contact your Administrator.

Automated Data processing



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.