1 ADP Boulevard
Roseland, N.J. 07068

Date: December 3, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "AUTOMATED DATA PROCESSING"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: **<Display Name<AT>nsula[.]edu>** with the following subject line: "**AUTOMATED DATA PROCESSING**". These emails instruct the recipient to click on a link to restore access to their ADP services.

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

Message Subject:
AUTOMATED DATA PROCESSING

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: @nsula.edu>
Sent: Tuesday, December 3, 2019 10:35 AM
Subject: AUTOMATED DATA PROCESSING

Hello,

For security and privacy related issues your access to the following services have been disabled on ADP workforcenow.

- Payroll
- Hiring
- Health & Benefits
- Security management
- Human Resources Administration
- Retirement Services
- Reports

For details about this notification visit your message center http://workforcenow.adp.com

Click below for instructions on how to restore access to your service(s):

https://workforcenow.adp.com/landing_remote/login.do?trnid=004UWBZQK3FXLOQAGHSF

If you have questions about this message, please contact your administrator.

Please do not reply to this message. Replies will not be received.

Thanks!

ADP, the ADP logo, and Always Designing for People are trademarks of ADP, LLC.

1 ADP Boulevard
Roseland, N.J. 07068

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.

ADP, the ADP logo, and Always Designing for People are trademarks of ADP, LLC.