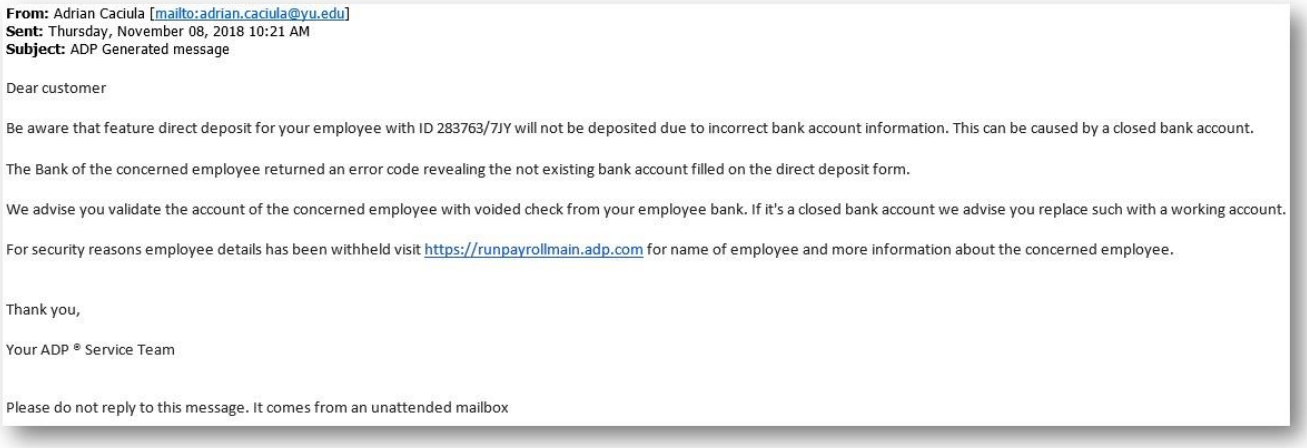
1 ADP Boulevard
Roseland, N.J. 07068

A more human resource.®

Date: November 8, 2018
From: ADP Global Security Organization
Subject: Phishing Campaign: “ADP Generated message”

ADP has received reports regarding fraudulent emails from adrian.caciula@yu.edu with the subject line “ADP Generated message”. These emails include a link and instruct the recipient to click on it.

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.



From: Adrian Caciula [mailto:adrian.caciula@yu.edu]
Sent: Thursday, November 08, 2018 10:21 AM
Subject: ADP Generated message

Dear customer

Be aware that feature direct deposit for your employee with ID 283763/7JY will not be deposited due to incorrect bank account information. This can be caused by a closed bank account.

The Bank of the concerned employee returned an error code revealing the not existing bank account filled on the direct deposit form.

We advise you validate the account of the concerned employee with voided check from your employee bank. If it's a closed bank account we advise you replace such with a working account.

For security reasons employee details has been withheld visit https://runpayrollmain.adp.com for name of employee and more information about the concerned employee.

Thank you,

Your ADP ® Service Team

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

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.