1 ADP Boulevard
Roseland, N.J. 07068

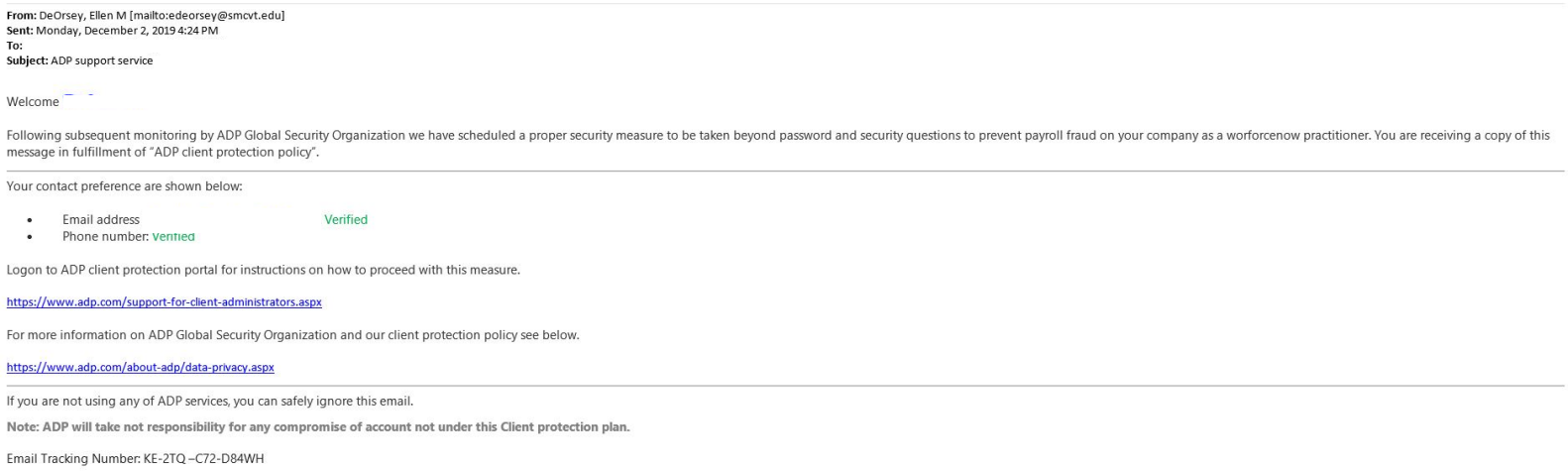
Date: December 3, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP support service"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: **DeOrsey, Ellen M <edeorsey><AT>smcvt[.]edu>** with the following subject line: "**ADP support service**" These emails instruct the recipient to sign in to their account to verify their information. The link takes the user to a cloned ADP login page.

Message Sender:
DeOrsey, Ellen M **<edeorsey><AT>smcvt[.]edu>**

Message Subject:
ADP support service

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: DeOrsey, Ellen M [mailto:edeorsey@smcvt.edu]
Sent: Monday, December 2, 2019 4:24 PM
To:
Subject: ADP support service

Welcome

Following subsequent monitoring by ADP Global Security Organization we have scheduled a proper security measure to be taken beyond password and security questions to prevent payroll fraud on your company as a worforcenow practitioner. You are receiving a copy of this message in fulfillment of "ADP client protection policy".

Your contact preference are shown below:

- Email address Verified
- Phone number: Verified

Logon to ADP client protection portal for instructions on how to proceed with this measure.

https://www.adp.com/support-for-client-administrators.aspx

For more information on ADP Global Security Organization and our client protection policy see below.

https://www.adp.com/about-adp/data-privacy.aspx

If you are not using any of ADP services, you can safely ignore this email.

Note: ADP will take not responsibility for any compromise of account not under this Client protection plan.

Email Tracking Number: KE-2TQ –C72-D84WH

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.

Sign up to have new alert notifications delivered to you by email – visit the alerts section of www.adp.com/Trust for more information.