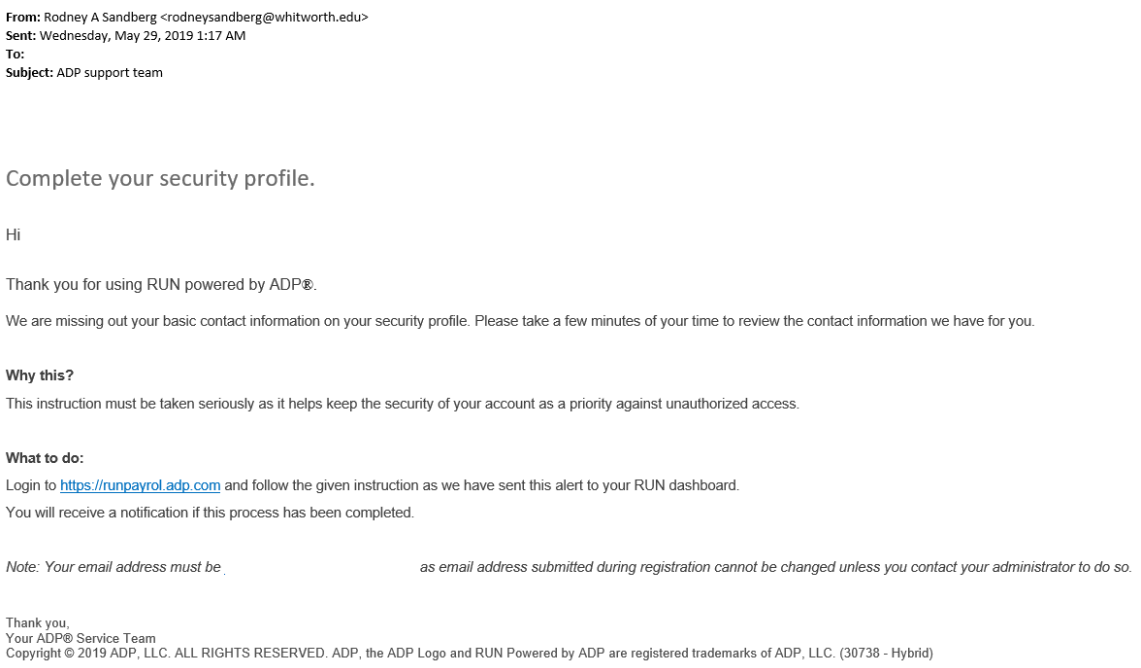
1 ADP Boulevard
Roseland, N.J. 07068

Date: June 3rd, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: “ADP Support Team”

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format : “Rodney A Sandberg <rodneysandberg@whitworth.edu>” with the subject line “**ADP support team**”. These emails instruct the recipient to click on a link in order to fill in their contact information on their security profile. The link redirects the user to a phishing page.

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: Rodney A Sandberg <rodneysandberg@whitworth.edu>
Sent: Wednesday, May 29, 2019 1:17 AM
To:
Subject: ADP support team

Complete your security profile.

Hi

Thank you for using RUN powered by ADP®.

We are missing out your basic contact information on your security profile. Please take a few minutes of your time to review the contact information we have for you.

Why this?

This instruction must be taken seriously as it helps keep the security of your account as a priority against unauthorized access.

What to do:

Login to https://runpayrol.adp.com and follow the given instruction as we have sent this alert to your RUN dashboard.

You will receive a notification if this process has been completed.

Note: Your email address must be as email address submitted during registration cannot be changed unless you contact your administrator to do so.

Thank you,
Your ADP® Service Team
Copyright © 2019 ADP, LLC. ALL RIGHTS RESERVED. ADP, the ADP Logo and RUN Powered by ADP are registered trademarks of ADP, LLC. (30738 - Hybrid)

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 spam2@adp.com.
- Delete the original email once you’ve received confirmation of receipt from spam2@adp.com.
- If you clicked any link or opened an attachment in the email, immediately contact your local IT support team for further action.
- If you receive external inquiries regarding this email, please advise the email is fraudulent and should be deleted. If the recipient opened an attachment or link, they should contact their IT support.

1 ADP Boulevard
Roseland, N.J. 07068

Security Resources

- Subscribe to Security Wire on ADPworks for security updates and alerts.
- Visit the GSO Services Portal for security contacts, materials, policies, and more.