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.

---

**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.
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.