

Date: February 13, 2020
From: ADP Global Security Organization
Subject: Phishing Campaign: "Workforcenow"


ADP has received reports regarding fraudulent emails being sent to ADP clients with the following subject line "**ADP Workforcenow**". These emails instruct the recipient to click on a link in order to correct an error due to a security configuration within Workforcenow. The link redirects the user to a phishing ADP login page.


Message Sender:
Lorraine Brown <Lorraine.Brown<AT>health.utah.edu





Message Subject:
ADP Workforcenow

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.

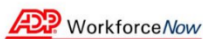
ADP Workforcenow

 Lorraine Brown <Lorraine.Brown@health.utah.edu>
To

 If there are problems with how this message is displayed, click here to view it in a web browser.

 Reply  Reply All  Forward 

Tue 2/11/2020 9:04

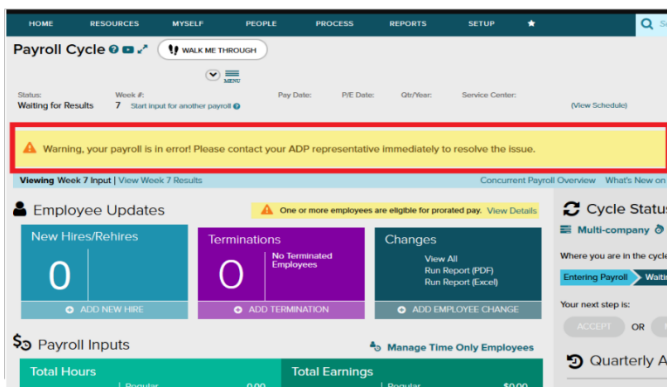


Hi there,

This is to notify you that ADP will not be paying your employees for your current pay period as your payroll is in error. This might have occurred due to violating security configuration rules as stated in ADP terms of use.

What happens if I submit my payroll?

Without taking required actions your payroll will not be processed as you will get an error message upon submitting your payroll. See below



What to do

Click the link to troubleshoot your ADP Workforcenow. You will get an email from ADP upon resolving this issue.

https://workforcenow.adp.com/theme/admin.html#/Process_ttd_ProcessTabPayrollCategoryPayrollCycle/ResolvePayrollError

If you are facing any difficulty resolving this issue please contact your administrator.

AUTOMATED DATA PROCESSING.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.



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.