

Date: December 3, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "Your ADP Payroll Invoice is ready!"

ADP has received reports regarding fraudulent emails being sent to ADP clients with the following subject line "**Your ADP Payroll Invoice is ready!**". The email instructs the recipient to click on a link to review a current invoice.

Message Sender:
ADP Payroll <aszmuc><AT>ao-chicago[.]com>

Message Subject:
Your ADP Payroll Invoice is ready!

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: ADP Payroll <aszmuc@ao-chicago.com>
Date: 11/27/19 16:10 (GMT-05:00)
To:
Subject: Your ADP Payroll Invoice is ready!

Your ADP Payroll invoice for last week is attached for your review.

If you have any questions regarding this invoice, please contact your ADP service team for assistance.

For security purpose the file is password protected: 000

Thank you for choosing ADP Payroll.

Important: Please do not respond 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.

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