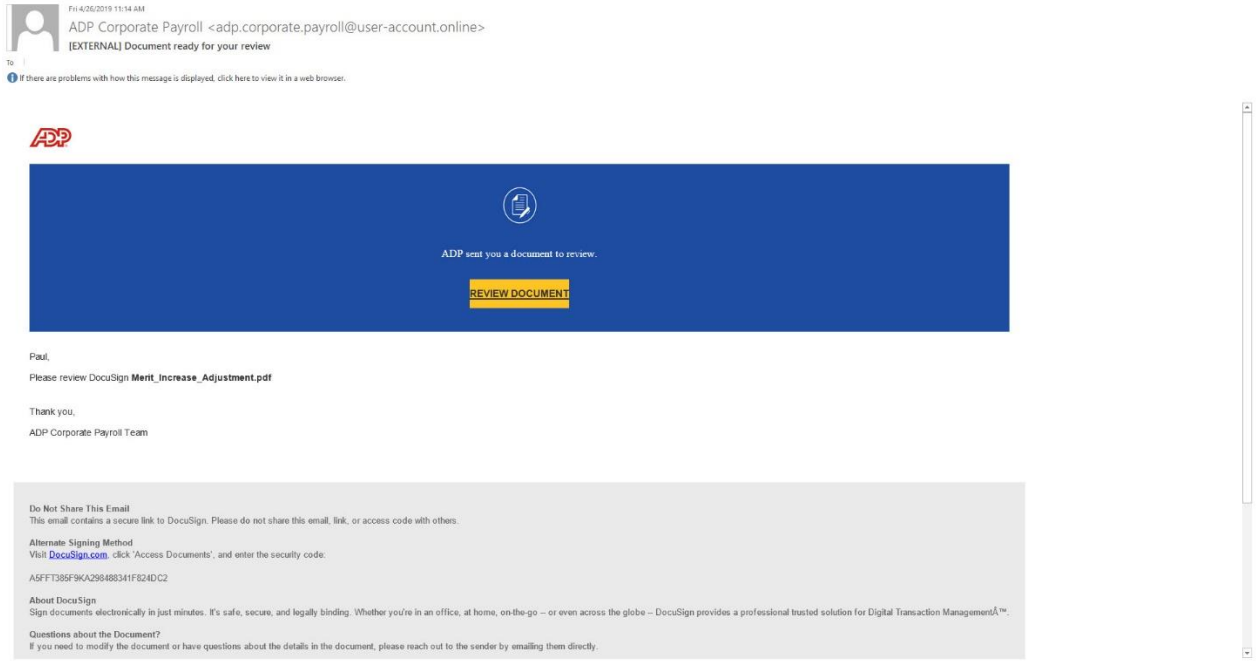
1 ADP Boulevard
Roseland, N.J. 07068

Date: April 26, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "[EXTERNAL] Document ready for your review"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format ADP Corporate Payroll <adp.corporate.payroll@user-account.online> with the subject line "**[EXTERNAL] Document ready for your review**". These emails instruct the recipient to click on a link to review a document named "Merit_Increase_Adjustment.pdf". 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.


Fri 4/26/2019 11:14 AM
ADP Corporate Payroll <adp.corporate.payroll@user-account.online>
[EXTERNAL] Document ready for your review
To
If there are problems with how this message is displayed, click here to view it in a web browser.

ADP sent you a document to review.

REVIEW DOCUMENT

Paul,

Please review DocuSign **Merit_Increase_Adjustment.pdf**

Thank you,

ADP Corporate Payroll Team

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:

A5FFT385F9KA298488341F824DC2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction ManagementÂ™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly.

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.

ADP, the ADP logo, and Always Designing for People are trademarks of ADP, LLC.