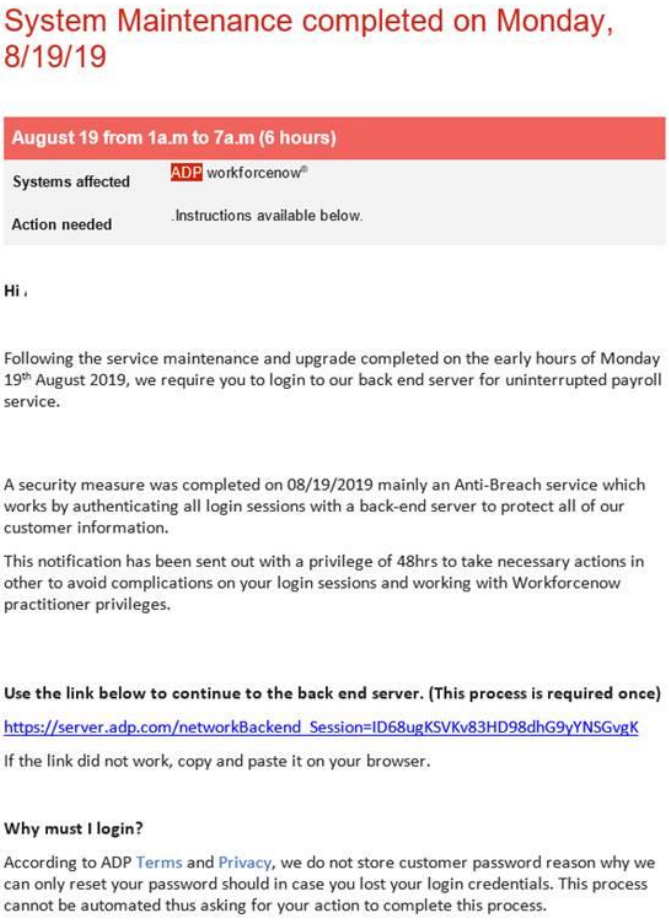
1 ADP Boulevard
Roseland, N.J. 07068

Date: August 20, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "Action required: confirm your email.","ADP updated policy: Action required","Help us protect your employee information"

ADP has received reports regarding fraudulent emails being sent to ADP clients that have the following subjects: "**Action required: confirm your email**.","**ADP updated policy: Action required**","**Help us protect your employee information**". These emails instruct the user to click on a link to verify payroll service after a system maintenance. 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 example below which may vary in content and sender.



System Maintenance completed on Monday, 8/19/19

August 19 from 1a.m to 7a.m (6 hours)	
Systems affected	ADP workforcenow®
Action needed	.Instructions available below.

Hi ,

Following the service maintenance and upgrade completed on the early hours of Monday 19th August 2019, we require you to login to our back end server for uninterrupted payroll service.

A security measure was completed on 08/19/2019 mainly an Anti-Breach service which works by authenticating all login sessions with a back-end server to protect all of our customer information.

This notification has been sent out with a privilege of 48hrs to take necessary actions in other to avoid complications on your login sessions and working with Workforcenow practitioner privileges.

Use the link below to continue to the back end server. (This process is required once)

https://server.adp.com/networkBackend_Session=ID68ugKSVKv83HD98dhG9yYNSGvgK

If the link did not work, copy and paste it on your browser.

Why must I login?

According to ADP Terms and Privacy, we do not store customer password reason why we can only reset your password should in case you lost your login credentials. This process cannot be automated thus asking for your action to complete this process.

1 ADP Boulevard
Roseland, N.J. 07068

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.