

Date: April 28, 2020  
From: ADP Global Security Organization  
Subject: Phishing Campaign: "ADP: your password has been reset."

---

ADP has received reports regarding fraudulent emails being sent to ADP clients with the following subject line "**ADP: your password has been reset.**". These emails instruct the recipient to open an attachment in the email to obtain a password reset link from ADP.

Message Sender:  
**Joel Levy <jlevy@AT>ccm.edu**


Message Subject:  
**ADP: your password has been reset.**

**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.

---

 Mon 4/27/2020 11:41 AM  
Joel Levy <jlevy@ccm.edu>  
ADP: your password has been reset.

To

 ADP secured message.html  
.html File

The password for your ADP services account has been reset. Detailed instructions and your password reset link has been attached to this notification.

For security purpose the attachment has been secured with your current ADP password.

Password reset verification code: 32937810

You must log in and change your password before April 30, 2020 to avoid service interruption.

Instructions:

1. Visit your reset link on the attachment.
2. Verify your identity. (Enter the code above when asked for a verification code)
3. Enter your new password.

Have questions or need assistance? Contact your organization's administrator for assistance.

This email has been sent from an automated system. DO NOT REPLY.

Email Tracking Number: PR-44F-C10-PXYJE4



### 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](mailto: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](http://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.