


Date: July 23, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP® support"

ADP has received reports regarding fraudulent emails being sent to ADP clients from multiple email addresses that have the following format : "name <at> capital<dot>edu" with the subject line "ADP® support" These emails instruct the recipient to click on a link to verify ADP two factor verification for improving security. 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.

Subject: ADP® support

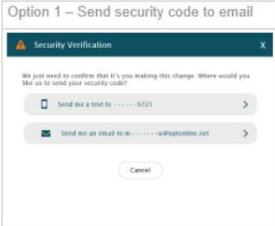
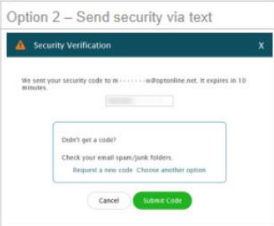


new and **improved** account security

Hi customer,

To better protect your company's information, we have implemented a **new two-factor verification process** in RUN Powered by ADP® (RUN). You or your administrator will be prompted to confirm your identity when making any changes to your account.

You'll have two options for verifying your identity:


Option 1 – Send security code to email	Option 2 – Send security via text
	

IMPORTANT – Actions you must take now:

1. [Login to RUN](#) and go to the Company tab.
2. Select My Security Profile.
3. Fill in your contact email address and your current phone number.
4. Follow the given procedures to complete this process.

Thanks for helping us keep your information safe!

Senior Administrator
Automatic data processing



Always Designing
for People™

Copyright © 2019 ADP, LLC. All Rights Reserved. ADP, the ADP Logo, Employee Access, and RUN Powered by ADP are registered trademarks, and ADP Always Designing for People is a trademark of ADP, LLC and/or its affiliates.



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.