Always Designing for People™

1 ADP Boulevard
Roseland, N.J. 07068

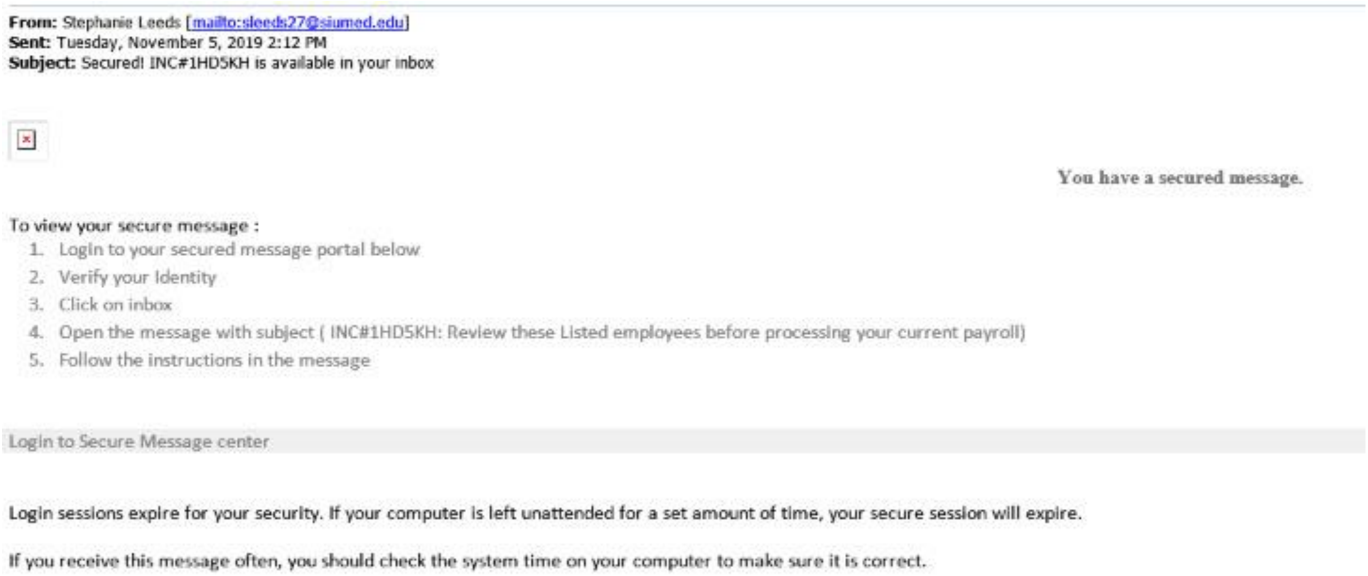
Date: November 6, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "Secured! INC #1HD5KH is available in your inbox"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: **<sleeds27><AT>siumed[.]edu>** with the following subject lines: "**Secured ! INC #1HD5KH is available in your inbox**" These emails instruct the recipient to sign in to their account. The link takes the user to a **WorkForceNow** cloned login page.

Message Sender:
<sleeds27><AT>siumed[.]edu>

Message Subject:
"Secured ! INC #1HD5KH is available in your inbox"

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: Stephanie Leeds [mailto:sleeds27@siumed.edu]
Sent: Tuesday, November 5, 2019 2:12 PM
Subject: Secured! INC#1HD5KH is available in your inbox

You have a secured message.

To view your secure message :

1. Login to your secured message portal below
2. Verify your Identity
3. Click on inbox
4. Open the message with subject (INC#1HD5KH: Review these Listed employees before processing your current payroll)
5. Follow the instructions in the message

Login to Secure Message center

Login sessions expire for your security. If your computer is left unattended for a set amount of time, your secure session will expire.

If you receive this message often, you should check the system time on your computer to make sure it is correct.

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.