1 ADP Boulevard
Roseland, N.J. 07068

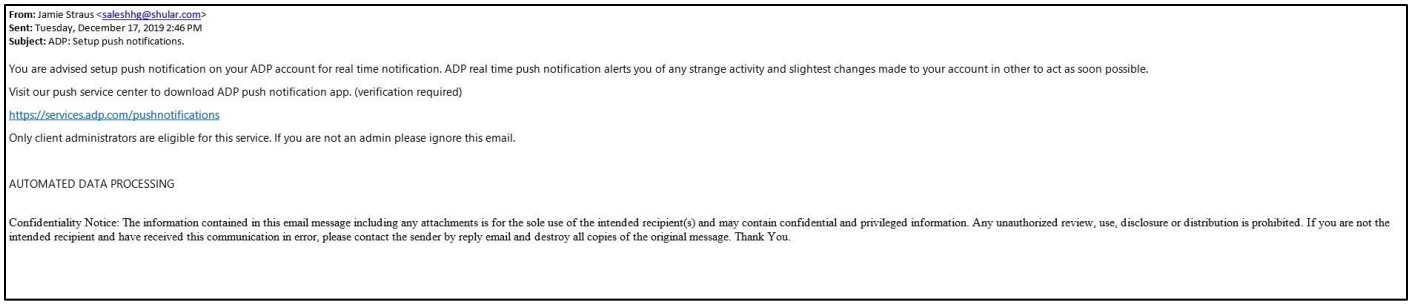
Date: December 18, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP: Setup push notifications"//"SECURITY GENERATED MESSAGE"

ADP has received reports regarding fraudulent emails being sent to ADP clients that have the following subjects: "**ADP: Setup push notifications**" and "**SECURITY GENERATED MESSAGE**". The email instructs the user to click on a link to sign in to their ADP account. The link takes the user to a fake **RUN** or **WFN** page, the credentials entered are then stolen.

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.

Message Sender:
Jamie Straus<saleshhg><AT>shular[.]com>
Cat Drube<cdrube><AT>shular[.]com>

Message Subject:
"**ADP: Setup push notifications**"
"**SECURITY GENERATED MESSAGE**"



From: Jamie Straus <saleshhg@shular.com>
Sent: Tuesday, December 17, 2019 2:46 PM
Subject: ADP: Setup push notifications.

You are advised setup push notification on your ADP account for real time notification. ADP real time push notification alerts you of any strange activity and slightest changes made to your account in other to act as soon possible.

Visit our push service center to download ADP push notification app. (verification required)

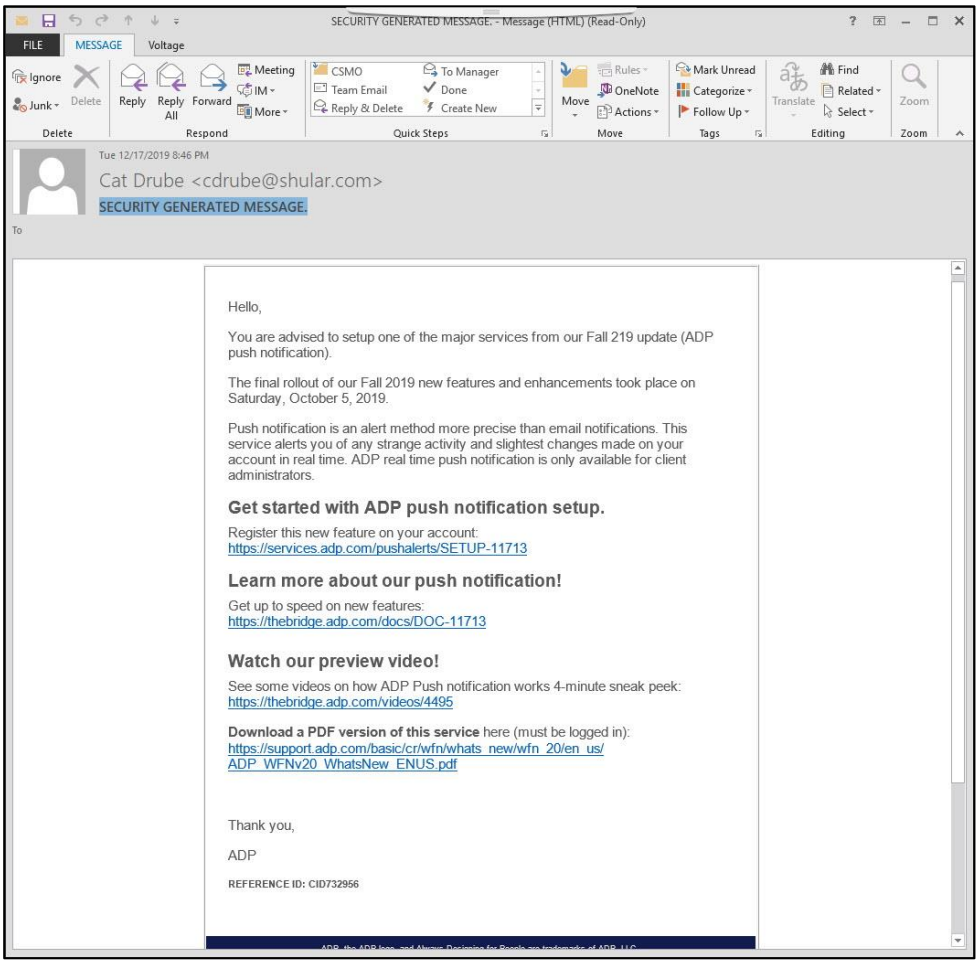
https://services.adp.com/pushnotifications

Only client administrators are eligible for this service. If you are not an admin please ignore this email.

AUTOMATED DATA PROCESSING

Confidentiality Notice: The information contained in this email message including any attachments is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient and have received this communication in error, please contact the sender by reply email and destroy all copies of the original message. Thank You.

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.

Sign up to have new alert notifications delivered to you by email – visit the alerts section of www.adp.com/Trust for more information.