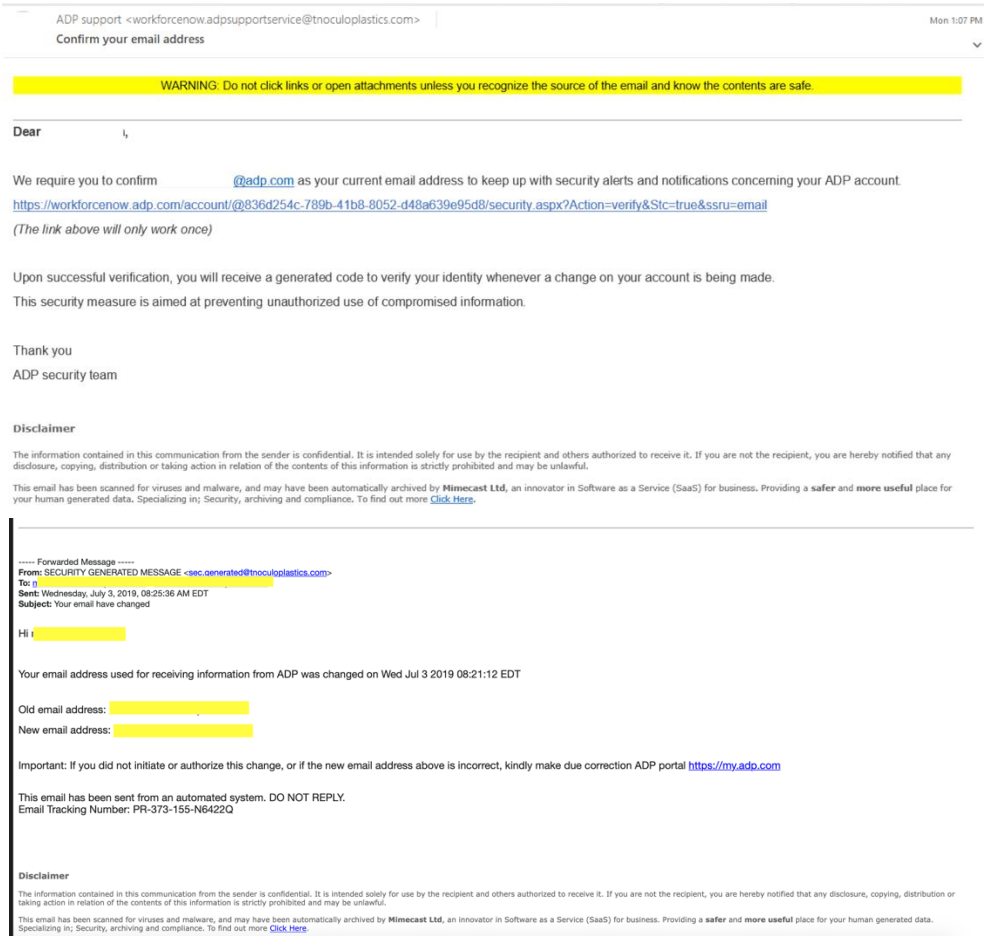
1 ADP Boulevard
Roseland, N.J. 07068

Date: July 19, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "Please provide an alternative." // "Your email have changed"//"Your security preference has been reset"//"Confirm your email address"

ADP has received reports regarding fraudulent emails being sent to ADP clients that have the following subjects: "**Please provide an alternative.**", "**Your email have changed**", "**Your security preference has been reset**" or "**Confirm your email address**". Please note that we reported a similar phishing campaign on June 6th and July 4th - the sender address varies but is consistently ***XXX@tnoculoplastics.com***. All emails include links posing as ADP login pages.

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.



ADP support <workforcenow.adpsupportservice@tnoculoplastics.com> Mon 1:07 PM
Confirm your email address

WARNING: Do not click links or open attachments unless you recognize the source of the email and know the contents are safe.

Dear ,

We require you to confirm @adp.com as your current email address to keep up with security alerts and notifications concerning your ADP account.
https://workforcenow.adp.com/account/@836d254c-789b-41b8-8052-d48a639e95d8/security.aspx?Action=verify&Stc=true&ssru=email
(The link above will only work once)

Upon successful verification, you will receive a generated code to verify your identity whenever a change on your account is being made.
This security measure is aimed at preventing unauthorized use of compromised information.

Thank you
ADP security team

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

----- Forwarded Message -----
From: SECURITY GENERATED MESSAGE <sec.generated@tnoculoplastics.com>
To:
Sent: Wednesday, July 3, 2019, 08:25:36 AM EDT
Subject: Your email have changed

Hi

Your email address used for receiving information from ADP was changed on Wed Jul 3 2019 08:21:12 EDT

Old email address:
New email address:

Important: If you did not initiate or authorize this change, or if the new email address above is incorrect, kindly make due correction ADP portal https://my.adp.com

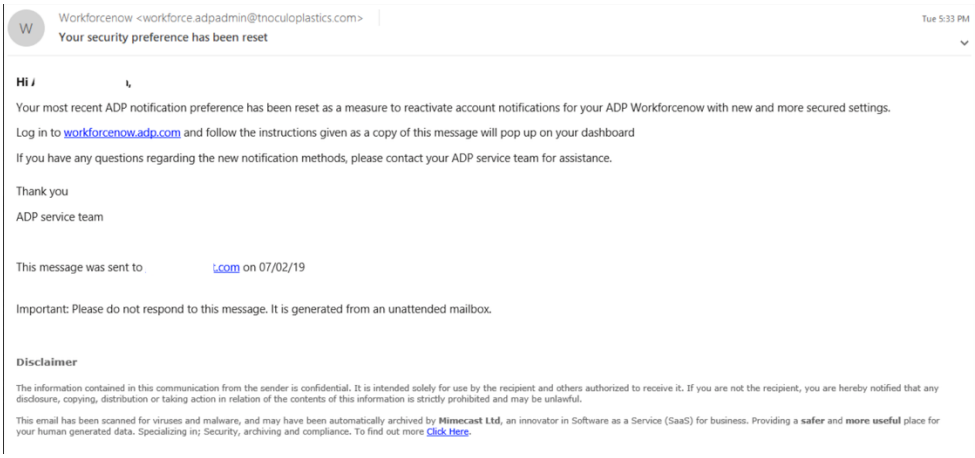
This email has been sent from an automated system. DO NOT REPLY.
Email Tracking Number: PR-373-155-N6422Q

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

1 ADP Boulevard
Roseland, N.J. 07068



W Workforcenow <workforce.adpadmin@tnoculoplastics.com> Tue 5:33 PM

Your security preference has been reset

Hi ,

Your most recent ADP notification preference has been reset as a measure to reactivate account notifications for your ADP Workforcenow with new and more secured settings.

Log in to workforcenow.adp.com and follow the instructions given as a copy of this message will pop up on your dashboard

If you have any questions regarding the new notification methods, please contact your ADP service team for assistance.

Thank you

ADP service team

This message was sent to .com on 07/02/19

Important: Please do not respond to this message. It is generated from an unattended mailbox.

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

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.