ADP has received reports regarding fraudulent emails being sent to ADP clients with the email address "ED BEN (admin) <ED.admin@tnoculoplastics.com>" with the following subject: "Complete the following registration". The email introduces a new ADP service named ADP TotalPay iNET where processed payroll and checks can be reversed and stopped for security purpose and adequate correction. The email has a link where the client can sign-up for this service.

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.

---

**Example Email**

From: ED BEN (admin) [mailto:ED.admin@tnoculoplastics.com]
Sent: Wednesday, August 7, 2019 10:46 AM
To: [Redacted]
Subject: Complete the following registration

Introducing ADP TotalPay iNET – a service where processed payroll and checks can be reversed/stopped for security purpose and for adequate correction.

This service which was originally exclusive to our clients needs to be run on behalf of your company by ADP providing adequate financial tracking and total control of your cash flows in your business.

**How to sign up for TotalPay iNET**
1. Visit the ADP Net Admin portal: [https://apn.adp.com](https://apn.adp.com)
2. Login to verify your identity.
3. Click "Register as a new user"
4. Complete the few steps required.

**How to stop unauthorized processed payroll/checks:**

Upon successful completion of the sign up process, you can:
1. Click on COMPANY on your top bar of the Payroll dashboard.
2. Select TotalPay iNET.
3. Enter Check Date or Check Number of concerned payroll to search.
4. Select Stop payment.

**NOTE:** To stop payment for every employee under the selected payroll, click on Stop Full Payroll else select from the dropdown of the employee listed.

**Type of TotalPay iNET users:**

TPNetAdmin (Networks)

- User authorized by the client to add/delete users, change passwords, or remove certificates.

TPNetClientAdmin.

- The TPNetClientAdmin can manage all users and can create TPNetAdmin, TPNetUsers, and TPNetReporters, reset passwords, and process ADPCheck (Stop payment, FSOO deletion/reversal, ADPCheck copy requests, and reports requests). TPNet Admin.

TPNetUser.

- These users can process and view status of ADPCheck stop payment, FSOO deletion/reversal, ADPCheck copy requests, and report requests.

Thank you

ADP SERVICE

The ADP logo is a registered trademark of ADP North America, Inc. All other trademarks and service marks are the property of their respective owners. T&SM 04-08-06

TotalPay iNET Web (for Employers), August 2019

---

Disclaimer:

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

This email has been approved for review 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.