

Date: August 29, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: "ADP Support"

ADP has received reports regarding fraudulent emails being sent to ADP clients with the email address "**Vahe (Vic) Novshadyan <VNovshadyan<at>centennialcollege<dot>ca**" with the following subject: "**ADP Support**" The email instructs the user to click on a link to review updated user policies and verify their email address. 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.

From: Vahe (Vic) Novshadyan <VNovshadyan@centennialcollege.ca>
Sent: Wednesday, August 28, 2019 9:52 PM
Subject: [SPAM] ADP support

Verify your email address

We are asking you to verify your email address in accordance to our updated user policy.

**Follow the link below to verify your email address.
This link will only work once.**

<https://verifyemail.adp.com/token=@526d254c-33b-41b8-8052-d43a639e95d8>

If you cannot use the link, copy and paste the link into a browser.

Once you have followed the link, you should delete this temporary message, which is used only to verify your email address.

Keep the original encrypted message for access in the future

We're here to help! Please contact your ADP Representative for any questions you may have.

NOTE: This email is from an unattended mailbox, please do not reply.

This mail is intended solely for the use of the individual to whom it is addressed and may contain information that is privileged, confidential, or otherwise exempt from disclosure. If the reader of this mail is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this notification in error or would like to make changes to your preferences, please visit your ADP SmartCompliance® "Notification Preferences" page.

ADP and the ADP logo are registered trademarks of ADP, LLC. ADP A more human resource is a service mark of ADP, LLC. All other marks are the property of their respective owners. Copyright © 2019 ADP, LLC. All rights reserved.



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.