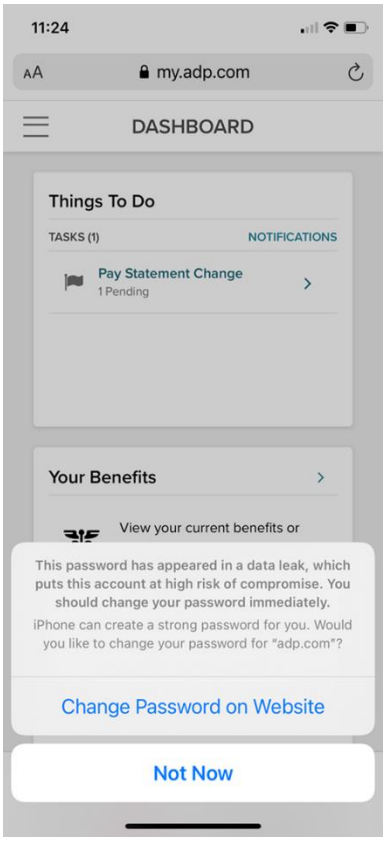
1 ADP Boulevard
Roseland, N.J. 07068

Date: October 28, 2020
From: ADP Global Security Organization
Subject: Compromised Password Alert on Mobile Devices

ADP has received some user inquiries regarding compromised password notifications that were received while logging onto ADP's services via a mobile device (refer to image to the right). The notification indicates that the password may be compromised and should be reset immediately.



ADP does not share user credentials and this notification is not an indicator that ADP was breached. At this time, ADP has determined that none of its internal systems have been compromised and no intrusion has occurred. Further, this notification only applies to Apple device users operating on iOS 14.

Background

With the release of iOS 14, a new feature was introduced that notifies users when their stored passwords have been compromised. To do this, Safari uses strong cryptographic techniques to regularly check derivations of passwords against a list of breached passwords in a secure and private way that doesn't reveal the user's password information to the website they are trying to log into or even to Apple.

Why A User Would Receive This Notification

If a user receives this notification while attempting to log into an ADP service, it could be an indicator that iOS 14's algorithm has compared the password the user entered against a breached-password database and has determined that its likely the password has been compromised in the past. ADP does not share client or user information with Apple and has no way of knowing how or why the password is flagged.

Recommended Actions

Out of an abundance of caution, ADP recommends that users that receive this notification select "Not Now" and go directly to their ADP account to change their password. Do not change your password through the "Change Password on Website" option as you will be directed to www.adp.com and not your applications' log-in page.

Further, we recommend that users refer to the publicly available website, www.haveibeenpwned.com to verify if and where their credentials may have been compromised. Please note that ADP is not affiliated with this website in any way.

ADP's layered defense includes technologies and controls to identify and/or prevent these types of threats, including assessing vulnerabilities and applying appropriate protection and detection control updates.
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.