

Date: Tuesday, March 23, 2021
From: ADP Global Security Organization
Subject: Phishing Campaign: Your Intuit Account Has Been Put On Hold; ADP Security

ADP has received reports about fraudulent emails sent to ADP clients. 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:

ADPpayment<AT>ADPsolutions[.]com
ADPalert<AT>ADPalert[.]com
ADPalert<AT>adpsecurityalert[.]com
ADPalert<AT>ADPsecurealert[.]com
ADPsecurity<AT>adpsecure[.]com

Message Subject:

"Your Intuit Account Has Been Put On Hold"
"Your Account Has Been Put On Hold"
"Final Warning:Your Account Has Been Put On Hold"
"Account Suspension Notice"
"Final Warning: Account Suspension Notice!"

Dear User,

Thank you for choosing ADP Payment Solutions. A temporary hold has been placed on your account due to recent activities.

You have been subjected to verification in order to restore your Account .

Kindly Logon below to begin

www.adp.com

Thank You,
Intuit Team



Dear User,

Thank you for choosing ADP Payment Solutions. A temporary hold has been placed on your account due to recent activities.

You have been subjected to verification in order to restore your Account .

Kindly Logon below to begin

[RESTORE YOUR ACCOUNT](#)

Thank You,
ADP Team

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 spam2@adp.com.
- Delete the original email once you've received confirmation of receipt from spam2@adp.com.
- If you clicked any link or opened an attachment in the email, immediately contact your local IT support team for further action.
- If you receive external inquiries regarding this email, please advise the email is fraudulent and should be deleted. If the recipient opened an attachment or link, they should contact their IT support.

Security Resources

- Visit [Security Hub](#) for security alerts, contacts, materials, policies, and more.
- Subscribe to [Security Wire](#) on ADPworks for security updates.

