STELLANTIS

COMPANY VEHICLE OPERATIONS

Dear Eligible Participant,

We are writing as a follow up to our recent email regarding phishing scams. We are aware of an active phishing scam where participants may be contacted by email or phone from someone pretending to be from Company Vehicle Operations asking to have money sent to them.

Please use caution anytime you receive an email or phone call asking you to send money. Company Vehicle Operations will always request that money be sent directly to us only at our Lapeer Road Marshaling Center address at 4300 S. Lapeer Road, Orion Township, MI 48359.

If you believe you have been contacted by a scammer, please contact us:

Phone: 1-800-481-6736
NBU Active Employees and Retirees: cocars@stellantis.com
UAW-Represented Employees: uawvehicles@stellantis.com

As a reminder, please review the following information about cyberattacks, including phishing scams.

Phishing scams are a type of cyberattack where an attacker sends an email encouraging a user to download an attachment, click a link or send money. The attachment or link could install malware on the user's system to steal information and even the user's identity.

These emails may come from an email address that looks very similar to a legitimate email address, often having a different domain name (the part of the email address after the "@" sign) than the legitimate email address.

Company Vehicle Operations will always send an email from a corporate email domain such as "@stellantis.com." For example: cocars@stellantis.com, uawvehicles@stellantis.com etc. Some Stellantis system generated emails may have "Company Vehicle Operations<DoNotReply@americas.stellantis.com" or "@chrysler.com" as the domain.

There are some additional things you can do to spot cyberattacks and help protect yourself and Stellantis:

- Do not click any links, do not open any attachments from an email address you don't know or were not expecting. Check the sender's email address (including the domain) for legitimacy first. You can do this by hovering your mouse over the sender's email address (without clicking on it) to view the entire address, including the domain.
- Always check the URL before clicking a hyperlink by hovering over the link with your cursor.
- Active employees: to report a suspicious email received by your corporate email address (@stellantis.com) please forward it to the Cyber Security Stellantis Team at: phishing@stellantis.com.
- Look for spelling or grammar errors. Phishing emails frequently contain these errors but not always.

Thank you for your attention to this important security matter. And rest assured, we are working diligently to resolve the fraudulent activity and appreciate your patience during this time.

Company Vehicle Operations

October 1, 2024