**Computer Emergency Response Team of Mauritius**
**Ministry of Information Technology, Communication and Innovation**

# CERT-MU Security Alert

**Date of Issue:** 09 October 2024

## Scams Alert

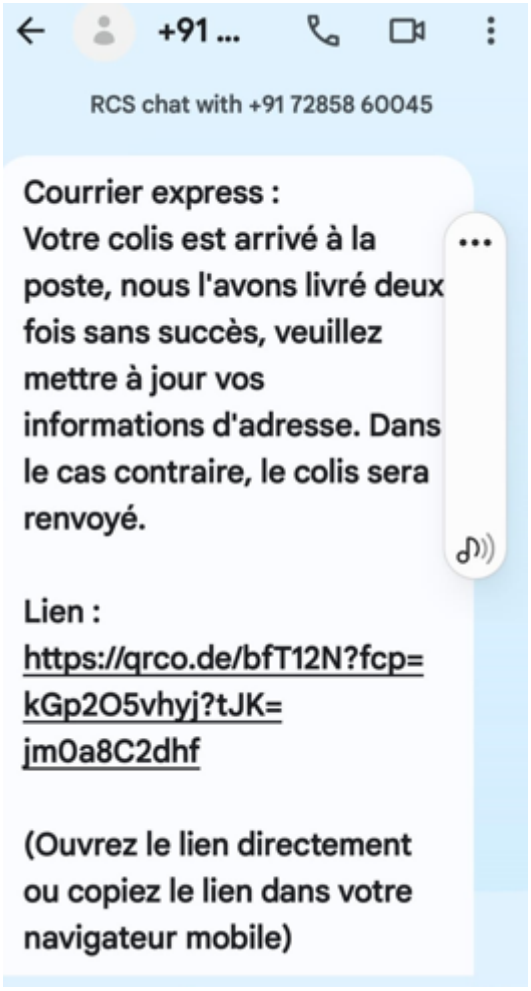
**Severity Level:** High

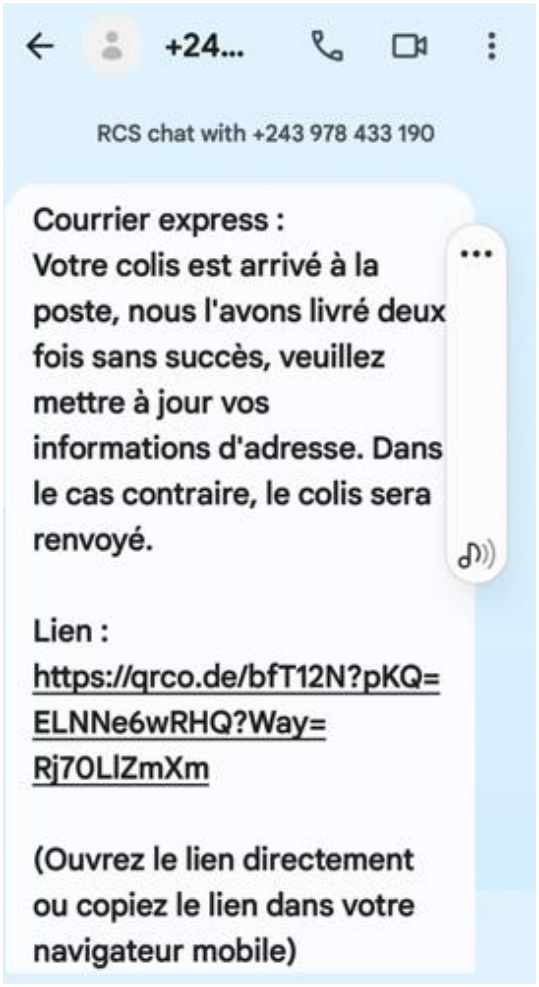
### Description:

CERT-MU has observed a recent surge in fraudulent text messages targeting individuals across the island. Scammers are posing as legitimate courier services, falsely claiming that a parcel addressed to you could not be delivered. The messages urge recipients to click on a provided link to update their delivery address. However, these links lead to phishing websites designed to steal personal information or infect devices with malware.

These scammers are exploiting the increased reliance on online shopping and courier deliveries. The fake messages are often crafted to appear urgent, pushing victims to act quickly without verifying the legitimacy of the claims. By creating a sense of urgency and using familiar terminology related to parcel delivery.

As seen in the screenshots below, two notable examples of the fraudulent messages include:




In both cases, a suspicious link to a fraudulent website is included, urging you to update your delivery address, which could lead to personal information theft.

**How This Scam Works:**

1. You receive a text message claiming that a parcel could not be delivered after multiple attempts.

2. The message includes a link for updating your delivery address or to provide additional details to "recover" your parcel.

3. If you click the link, it directs you to a fake website that either asks for personal information (such as credit card details, ID, or address information) or attempts to install malware on your device.

4. Once the scammers have your information, they can use it to commit identity theft, financial fraud, or sell your details to other cybercriminals.

**How to Protect Yourself:**

- Do not click on any links provided in unsolicited text messages or emails.
- Verify the legitimacy of the message by directly contacting the courier company using official contact details. Most courier services will not request sensitive information via text.
- Look for red flags, such as unknown international phone numbers, generic greetings, and suspicious URLs. Official websites often have recognizable domain names (e.g., .com, .mu).
- Report the message to CERT-MU or your mobile service provider as soon as possible. They can take further steps to investigate and block similar scams.
- Regularly monitor your bank statements and credit card activity to spot any unusual or unauthorized transactions.

If you have received such a message or accidentally clicked on a suspicious link, immediately report the incident to CERT-MU for assistance. We will help assess the situation and take necessary action to mitigate any potential damage.

## Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

## Contact Information

**Computer Emergency Response Team of Mauritius (CERT-MU)**
**Ministry of Information Technology, Communication and Innovation**
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org