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

CERT-MU Security Alert

Date of Issue: 30 October 2026

Beware of Fake Divali Cash Gift Scams Circulating on WhatsApp

Severity Level: High

Description:

CERT-MU is alerting the public about a fraudulent message currently circulating on WhatsApp, falsely claiming that the Prime Minister of Mauritius is offering a cash gift of Rs. 2,000 to everyone in Mauritius to celebrate Divali.



To claim the alleged cash gift, users are lured to click on the "View Now" button. This redirects them to a suspicious website that prompts them to provide personal information. The fraudulent advertisement also displays the logos of local telecommunications operators such as MyT, Emtel and Chili to create an impression of legitimacy.

CERT-MU strongly advises members of the public **NOT TO CLICK** on the fraudulent link or provide any personal, banking or financial information. The link may lead to malicious websites designed to steal sensitive information and compromise users' personal and financial security.

Stay Alert During the Festive Season

As Mauritius approaches the festive season, cybercriminals may increasingly exploit festive celebrations and public enthusiasm by circulating fraudulent offers, fake giveaways, cash rewards, shopping promotions and other deceptive schemes through WhatsApp, social media and online platforms.

These scams often impersonate government authorities, well-known organisations or trusted brands to mislead unsuspecting individuals into clicking malicious links or disclosing sensitive information.

CERT-MU Advises the Public to:

1. Avoid clicking on suspicious links received through WhatsApp, SMS, social media or other messaging platforms, particularly those promising free cash gifts or rewards.
2. Verify the authenticity of offers through official government websites or the verified communication channels of the organisations concerned.
3. Never disclose sensitive information, including National Identity Card details, banking information, passwords, PINs or One-Time Passwords (OTPs).
4. Be cautious of offers that appear too good to be true, especially those promising easy money, festive giveaways or financial rewards.
5. Do not forward suspicious messages to friends, family members or WhatsApp groups, as this may contribute to the spread of fraudulent schemes.
6. Report suspicious messages and websites through the MAUCORS+ platform at https://maucors.govmu.org/.

Report Cyber Incidents

Report a cyber cybersecurity 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