



Computer Emergency Response Team of Mauritius
A Department under the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 17 July 2025

Beware: Fake TEMU Online Job Offers Trending on Social Media

Description

CERT-MU wishes to inform the general public that an online scam is circulating on social media and messaging platforms, falsely offering online work opportunities with the e-commerce platform TEMU. Several incidents have already been reported on MAUCORS+ in this regard.

The modus operandi of this scam are as follows:

1. Victims encounter social media advertisements promising easy online jobs with Temu.
2. Clicking on the advertisement redirects victims to WhatsApp chat with number +261 38 47 229 38.
3. The victim is instructed to contact a so-called "mentor" via Telegram at <https://t.me/dgo2654>.
4. The mentor requests the victim to register on the website: <https://netaoso.top/index/user/login.html> where he/she is asked to insert his/her phone number and invitation code to complete the tasks.
5. After registration, the victim is asked to carry out 8 tasks and is rewarded with Rs. 300, which can immediately be withdrawn.

TEMU

Job Vacancies

Available Job Vacancies Remote work via mobile phone

Chat and Messaging Assistant Reply to messages and provide customer service via WhatsApp or other applications Salary: 8 000 MUR	Social Network Manager Post content and follow comments on platforms such as Instagram, Facebook Salary: 15 000 MUR
Digital Surveyor Complete surveys or forms for market research via mobile phone Salary: 13 000 MUR	Online Sales Assistant Answer inquiries and complete sales via mobile phone in virtual stores Salary: 20 000 MUR

6. After that, the victim is instructed to recharge his/her account with Rs 300 in order to unlock further tasks.
7. The deposit of money is done to an **MCB Account via the Juice platform**.
8. After completing 13 additional tasks, a balance of Rs. 600 is shown in the victim's account. This completes the first round.
9. In the second round, when the victim reaches the 8th task, the platform blocks further progress with a message instructing them to recharge their account again to continue, effectively trapping them into a continuous payment loop.
10. When the victim tries to withdraw his/her money from the platform, it is shown "transactions pending" and scammers also cease communication with the victim.

Recommendations

CERT-MU advises users to be careful regarding such type of job offers, especially those trending on social media websites. It is also recommended to:

1. Verify Job Offers and Advertisements

- Always cross-check job opportunities directly on the official websites or verified social media pages of the company (e.g., Temu).
- Be cautious of offers that promise quick money with little effort.

2. Never Send Money Upfront

- Legitimate employers never ask for payments to process applications, unlock funds, or secure a job.

3. Avoid Unofficial Communication Channels

- Be suspicious if you are asked to continue conversations via personal WhatsApp numbers or Telegram accounts.
- Use only official communication platforms listed by the company.

4. Think Before You Click

- Do not click on suspicious links or ads shared on social media, especially those with unrealistic offers or high returns.

5. Verify Bank Account Requests

- Never transfer money to personal bank accounts of unknown individuals.
- Scammers often use bank accounts that appear to be local to build trust.

6. Report Suspicious Activities

- If you suspect a scam, report it immediately to:
 - CERT-MU via the MAUCORS+ platform (<https://maucors.govmu.org>)
 - The Cybercrime Unit of the Mauritius Police Force (210 4653)

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert.govmu.org

Website: <http://cert-mu.org.mu>

MAUCORS: <http://maucors.govmu.org>