CERT-MU Security Alert

Fake Email from the Mauritius Police Force

Issue Date: 02 May 2020

The CERT-MU has come across a Fake Email that seems to originate from the Mauritius Police Force (MPF) and which is targeting the citizens of Mauritius. The email has the subject: Fine due to curfew breach and it states that it was recorded by the Police that the recipient did not abide by the Curfew Order and left his/her house on 3 occasions and consequently is being fined the sum of Rs. xxx. The recipient is also requested to click on a link in the email to have more details.

A screenshot of the email is shown below for your reference:

CERT-MU wishes to inform the public in general that this is a Fake Email and does not originates from the Mauritius Police Force. A Fake email address (noreply@police-govmu.mu.com) has been used to trick and mislead the public. It is to be noted that the url “https://www.gov.mu.org/...” has been used to convince users about the genuineness of the email and upon clicking on it, it redirects recipient to another malicious phishing link.

It is advised NOT TO CLICK on the link as it can infect the recipient’s computer and NOT TO REVEAL any personal and banking information.
Be Safe from Phishing

The CERT-MU recommends the following precautionary measures to be taken to prevent you from becoming a victim of these phishing scams:

- Do not respond to calls or texts from unknown numbers, or any others that appear suspicious.
- Never share your personal or financial information via email, text messages, or over the phone.
- Be cautious if you are being pressured to share any information or make a payment immediately.
- Scammers often spoof phone numbers to trick you into answering or responding. Remember that government agencies will never call you to ask for personal information or money.
- Do not click any links in a text message. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they were not hacked.
- If you are unsure if an email, text or any other communication is genuinely from a legitimate source, do not click on the link or open the attachment. Contact the organisation via their official contact channels and ask.
- Protect your passwords and login credentials, do not enter these into any websites relating to the COVID-19 virus.
- Keep your devices up-to-date.
- Keep your anti-virus up to date and run regular checks.

Report Incidents

Let us unite together for a Safe Mauritian cyberspace during this crisis situation. In case you become victim to a scam, report the incident on the Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org).

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
Hotline No: (+230) 800 2378 | Fax No: (+230) 208 0119
Gen. Info.: contact@cert.ncb.mu | Incident: incident@cert.ncb.mu | Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org