National Computer Board

CERT-MU

CERT-MU Security Alert

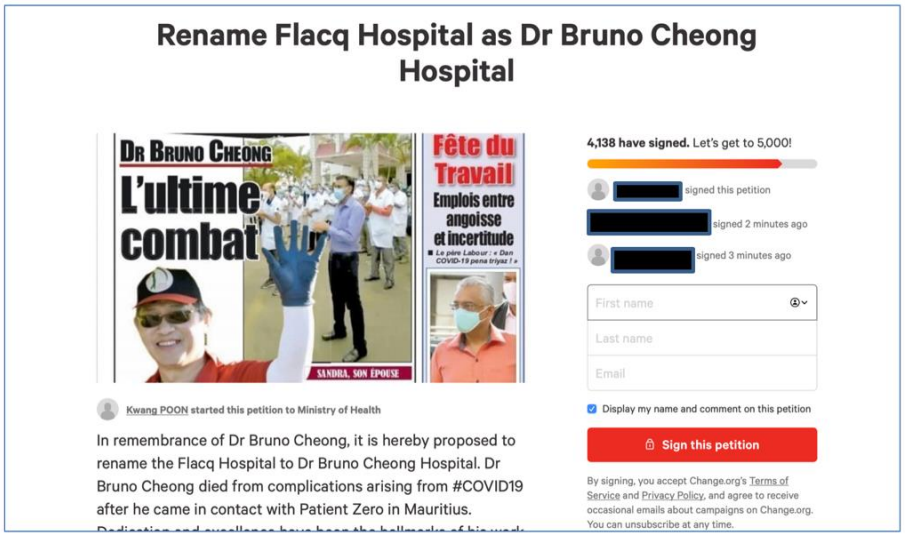
Petition Scam: Rename Flacq Hospital as Dr Bruno Cheong Hospital

Issue Date: 03 May 2020

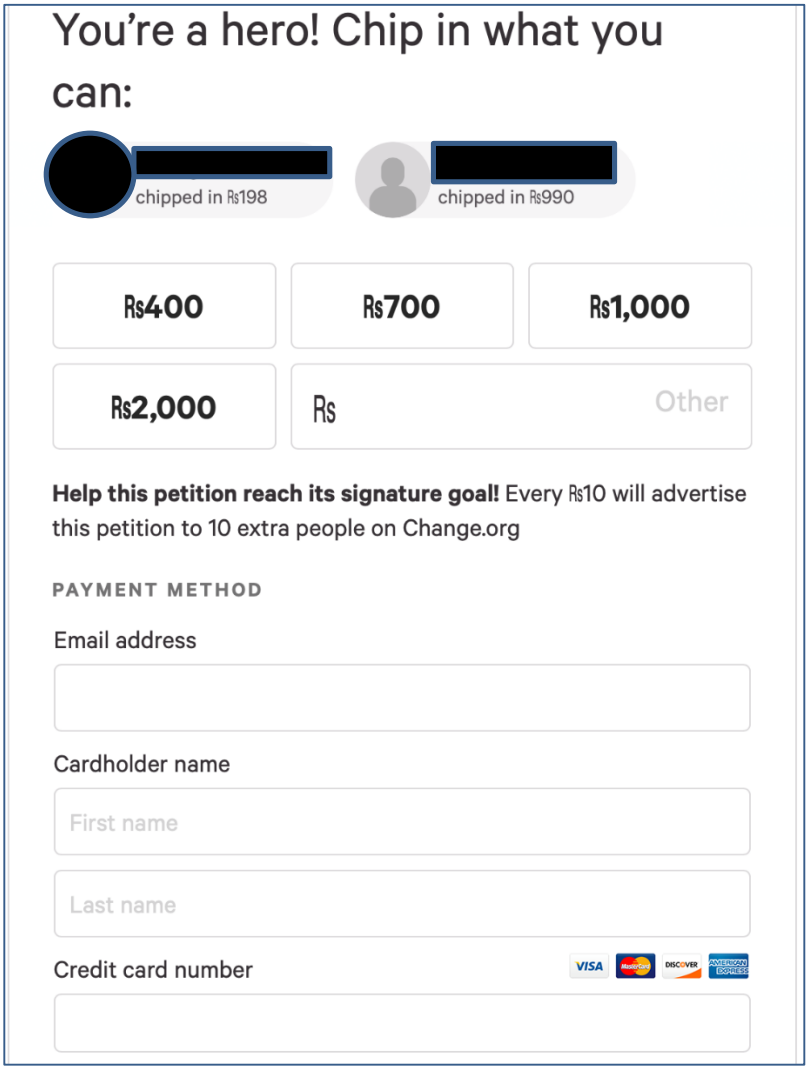
The CERT-MU has noted that a Petition "**Rename Flacq Hospital as Dr Bruno Cheong Hospital"** has been created on Change.org website (https://www.change.org/p/ministry-of-health-rename-flacq-hospital-as-dr-bruno-cheong-hospital), requesting people to sign the petition as a demand from the Government to change the name of the Flacq Hospital to Dr. Bruno Cheong Hospital. It is to be noted that someone who wishes to sign the Petition has to enter his personal information such as first name, last name and email address. After signing the Petition, the user is taken to another link where a donation is required. The donation can be in any amount, depending on the person. Social media platforms such as Facebook and WhatsApp are also being used to propagate this petition.

CERT-MU wishes to inform the public in general that this is a Petition scam and is being used by scammers as a good way to express concern about a critical issue or event, with the aim to gain sympathy of people and extract money from them in the form of charity.

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



Screenshot of donation window:



CERT-MU recommends the public in general to be cautious of these types of scams and do not reveal any personal/sensitive or banking information as this could lead to identity theft and monetary loss.

Be Safe from these scams

CERT-MU recommends the following precautionary measures to be safe from these 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