National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Incident Reporting Guideline Post Lockdown

Guidelines to Report an Incident to CERT-MU:-

CERT-MU provides information and assistance to the general public and organisations in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur.

What can I report to CERT-MU?

Incidents that are reported include phishing, hacking, denial of service, malicious code (malware, viruses, ransomware), website defacement, online scams, spamming, unauthorised access, compromised email accounts, sextortion, identity theft, and attacks on computer systems and any other cyber security related incidents.

Incident Reporting Channel

- To maintain social distancing due to the COVID-19 pandemic in Mauritius, incidents can be reported **ONLY** on the Mauritian Cybercrime Online Reporting System (MAUCORS - http://www.maucors.govmu.org), until further notice.

- The public in general and organisations are requested to follow the reporting guidelines on MAUCORS (http://maucors.govmu.org/English/Reporting/Pages/default.aspx) to report an incident.

- Enquiries about incidents can be made through CERT-MU Hotline: **800 2378 (between 8:45-16.00 hrs)**

- When reporting an incident online, users should also provide the following information if relevant to the nature of incident:

  Examples:
  - Fake or hacked accounts – name of the account and URL
  - Compromised Email accounts – User ID
  - Stolen pictures – screenshots
  - Online Scams - screenshots
  - Phishing – Phishing link, phishing email, email headers

  - Denial of Service or Distributed Denial of service attack – IP address
  - Unauthorised access – logs
  - Malware – malicious file, link or email
  - Website defacement – website link
  - Unauthorised video – link of video
  - Spam – email header

- The incident reporting party should preserve all the available information without any alteration.
- Incidents should not be reported from a machine which you think is infected.

What happens after reporting the incident?

After reporting the incident, the incident reporting party will receive an acknowledgement email with a ticket number. The ticket number can be used for further enquiries.

The reporting party will be informed when the incident is resolved or any other information or clarification is required or when the incident is transferred to any relevant authority.

What should not be reported to CERT-MU?

The following IT issues should **NOT** be reported to **CERT-MU**:

- Forgotten passwords or blocked / locked accounts
- VOIP services not working correctly (e.g Skype)
- Websites access issues (website is not loading properly)
- Internet connection problems
- Network problems
- Printer issues
- Any other non-cyber security related issue(s)

For legal actions, the reporting party should contact the Cybercrime Unit of the Mauritius Police Force.

12 May 2020

The Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
7th Floor, Stratton Court
La Poudriere Street
Port Louis