STEPS TO MITIGATE CYBER ATTACKS

1. As the national cyber defense institute, Sri Lanka CERT stands ready to help Government institutes prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to attacks of a similar nature.

2. Sri Lanka CERT recommends all Government institutes to adhere to following instructions in maintaining heightened posture when it comes to cybersecurity and protecting their most Critical Information Infrastructure.

a. Make sure, that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
b. Limit the administrative access right only to most important personal and ensure strong passwords being used.
c. Please inform the Head of your organization and all the staff to be extra vigilant on unusual emails and other links being sent to your mailing systems.
d. Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities.
e. Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for operational matters.
f. Firewalls and Web Application Firewalls will provide intruder detection and prevention measures to a great extent is the rules are properly programmed. Make sure that the threat databases are up to date.
g. If possible, please enable "geo blocking" in these devices if you do not expect any international traffic and allow only specific overseas traffic relevant to your business operations.
h. If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls against cloud security.
i. Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
j. Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
k. Designate a responsible individual to coordinate with Sri Lanka CERT for any suspected cybersecurity incident.
l. Assure availability of key personnel; identify means to provide immediate support for responding to an incident.

m. Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by a destructive cyberattack; ensure that backups are isolated from network connections.
n. Organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect organization's most critical assets in case of a cyber-attack.
o. Determine which systems were impacted, and immediately isolate them in case of a ransomware attack.
p. In case of any potential attack (Unavailability, defacement, etc.) being noticed, please contact Commander Nirosha Ananda (Retd.) – Chief Information Security Engineer (0763143287) for further assistance/ instructions.

These precautionary measures are prepared based on the recommended actions issued by Cyber Security & Infrastructure Security Agency (CISA), USA.