ISSUE NO 03

OCTOBER 2023

Cyber Guardian

A Publication on Online Safety

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

SECURITY

10 STEPS TO CYBER SECURITY

1. Risk Management Framework

It is essential to establish a risk management methodology in your organization with the involvement of senior management and the board of directors. Based on this methodology, assess the risks to your information and IT systems, and implement necessary controls to protect them.

2. Protect from Malware

Apply the latest security patches and securely configure all computers, systems, and other devices.

3. Security Configuration

Apply the latest security patches and securely configure all computers, systems, and devices.
Replace default passwords with strong passwords.

4. Removable Media

Be cautious when plugging external devices (USB/hard disk) into computers or networks. Scan for malware when connecting external devices.

5. User Education and Awareness

Most incidents are due to a lack of awareness in cybersecurity among individuals. Therefore, it is essential to have a program to make end users aware of the potential threats in cybersecurity.

6. Access Management

To prevent unauthorized access, it is essential to implement an access management policy within the organization. The details of the access management policy are presented in the Information and Cyber Security Policy for Government Organizations.(Visit www.cert.gov.lk) to download the policy.)

7. Backup

It is essential to back up your important data and logs regularly. Backups should be kept securely, and an air gap should be maintained between the live copy and backup data. The restorability of backups should be tested regularly.

8. Incident management

Establish an incident response plan for the organization and test the plan regularly.

9. Policy on Work from Home (Distance).

Develop a policy for working remotely and train staff to adhere to it. Establish secure connections and implement necessary technical controls to secure communication.

10. Security Aseessments

To identify vulnerabilities in information and IT systems, organizations should conduct security assessments of their IT systems and digital infrastructure periodically. Assessments should be performed before deployments, after making changes to systems, and after changes to hosting environments. Additionally, assessments should be conducted following the spread of malware or any incidents.

News

Sri Lanka CERT is conducting a series of workshops on cybersecurity (basics and advanced concepts) for Information Security Officers (ISO), Assistant Information Security Officers (AISO), and other government officers. The primary objective of these sessions is to educate participants on cybersecurity strategies and applications.

Sri Lanka CERT conducted a training session for newly appointed ICT teachers. This program was organized by Ministry of Education and nearly 230 ICT teachers representing all provinces participated for this event.

What does Sri Lanka CERT do?

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) is the National Center for Cyber Security, which has the national responsibility to protect the nation's cyberspace from cyber threats. It is currently operating under the Ministry of Technology.

Founded in 2006 as a state-owned enterprise, Sri Lanka CERT has grown into a globally-networked incident response center consisting of well-experienced and qualified cybersecurity professionals with a blend of multi-talented skills.

Sri Lanka CERT is a partner in global CERT networks, collaborating as a member of the international FIRST (Incident Response Forum), Asia Pacific CERT, Cyber4Dev European Union, and the World Bank to build a better cybersecurity ecosystem for the nation.

Sri Lanka CERT is committed to helping organizations and government agencies mitigate their impact by responding quickly to cyber-attacks such as ransomware or supply chain breaches in Sri Lanka. By constantly monitoring global cyber threats, technical support is also provided to educate the relevant parties and rescue them from threats. In addition, national cybersecurity policies and procedures are developed.

Circular

gov.lk
for Government Official Affairs

All government institutions must use official email addresses for their official communications. This official email should not be used for personal matters, as stated in the security and cybersecurity policy for government institutions.

This directive is further emphasized in circular SP/SB/10/13 issued by the President's Secretary. An official email is issued by the government under gov.lk. It is considered a government asset, and it is the responsibility of users to securely and responsibly use it.

New guidelines to protect Gmail users

Google is preparing to introduce new guidelines for e-mail senders to protect and strengthen e-mail against data theft and malicious malware software distribution by e-mail from next February. Thus, SPF/DKIM and DMARC authentication will be introduced for users' accounts to strengthen protection against email fraud and data theft.

It will help prevent data theft and hijacking and pinpoint the circulation of malicious software. To avoid annoying commercial emails, you can unsubscribe those communications by clicking one of the icons there. In addition, those commercial businesses have to take action to prevent contact within two days. Even now, Gmail's artificial intelligence-based security successfully prevents more than 99.9% of data theft and malware from contacting email, according to Google. Accordingly, it is possible to successfully block nearly 15 billion unwanted emails per day.

You don't have to worry about the intricacies of email security standards, but you have to be able to trust an email as a source. However, this will help email users to protect themselves from any vulnerabilities or potential threats.

Laws & policies

Laws and policies related to information, information technology & cyber security

- COMPUTER CRIME ACT, No. 24 OF 2007
- PAYMENT DEVICES FRAUDS ACT, No. OF 2006
- PERSONAL DATA PROTECTION ACT, No. 9 OF 2002
- ELECTRONIC TRANSACTIONS ACT, No. 19 OF 2006
- Information and Cyber Security Policy for Government Organizations 2003