ISSUE NO 01

AUGUST 2023

Cyber Guardian

Publication for your online safety

Policies

Sri Lanka CERT and the Ministry of Technology Join Forces to Implement Robust Information and

Cybersecurity Policy for Government Organizations

In a significant stride towards enhancing digital resilience and safeguarding sensitive information, Sri Lanka's Computer Emergency Readiness Team (Sri Lanka CERT) is collaborating closely with the Ministry of Technology to implement a comprehensive Information and Cybersecurity Policy for government organizations.

Key Collaborative Efforts

Cyber Threat Preparedness
Sri Lanka CERT, in partnership with the Ministry of Technology, is spearheading efforts to prepare government organizations against evolving cyber threats. This includes conducting vulnerability assessments threat analysis, risk assessments, and implementing proactive security measures.

Policy Framework
A robust policy framework is under development to establish clear guidelines, standards, and best practices for information security across government sectors. This framework will encompass data protection, incident response, and compliance.

Capacity Building
Training and capacity-building programs are being rolled out to equip government employees with the skills needed to detect and mitigate cyber threats effectively. This initiative promotes a culture of cybersecurity awareness.

Public-Private Synergy
Collaboration with the private sector and international cybersecurity entities strengthens Sri Lanka's cybersecurity posture. It fosters knowledge exchange, threat intelligence sharing, and resource optimization.

Empowering Government Organizations
The implementation of this policy is a vital step towards securing government data, services, and citizen information. It ensures a coordinated, proactive response to cyber incidents while fortifying Sri Lanka's digital landscape.

Engagement with Citizens
Sri Lanka CERT encourages citizens to play an active role in cybersecurity. Reporting suspicious online activities and practicing safe digital habits are integral to maintaining national cyber security.

In conclusion, the joint effort between Sri Lanka CERT and the Ministry of Technology underscores the government's commitment to cybersecurity. By embracing these policies and fostering a culture of cyber vigilance, Sri Lanka is positioning itself as a resilient and secure digital nation.

Security

Digital sentinels for Computer Security

In today's digital landscape, Virus Guards are essential for safeguarding your digital life. These programs, often known as antivirus software or security suites, serve as frontline defenders against computer viruses, malware, and cyber threats. Virus Guards continuously monitor your computer, detect and prevent malicious software in real-time. They get updated regularly to stay ahead of new threats, quarantine and remove detected threats, and provide firewall protection.

While Virus Guards are crucial, users must also exercise caution online, avoiding suspicious websites and attachments. Businesses, in particular, rely on these safeguards to protect sensitive data and maintain their reputation. Protecting sensitive data is important for both business and government organizations. One compelling reason for doing so is the preservation of their reputation.

In summary, Virus Guards serve as digital sentinels, safeguarding your devices and data in the constantly evolving digital landscape.

Risk

Risk of Insecure External data storage devices

In an age of digital convenience, External data storage devices (USB drives, external hard drives, etc.) have become ubiquitous tools for data transfer. However, their widespread use comes with inherent risks that demand our attention.

The Dangers of Insecure Usage

USB drives, while handy, can be a vector for malware and data breaches. When plugged into compromised computers, they can transfer malicious software, endangering your files and sensitive information.

Common Risks
Malware Transmission: Infected External drives can spread viruses, ransomware, or spyware from one device to another, causing significant damage.

Data Theft
Loss or theft of an external storage device can expose confidential data, potentially leading to identity theft or corporate espionage.

Mitigating Risks

To safeguard your digital assets:

Use Trusted Sources: Only use trustworthy external storage devices.
Regular Scanning: Regularly scan USB drives and external storage devices for malware with antivirus software.
Encrypt Data: Consider encrypting sensitive data on external storage devices to protect it from unauthorized access.
Educate Users: Promote awareness about the security of External data storage devices among employees or family members.

By being vigilant and adopting safe usage practices, we can minimize the risks associated with these ubiquitous devices.

Protect

How to protect your privacy in cyberspace

- Refrain from publicly sharing your email and other contact information.
- Review the settings of your social media accounts, including phone numbers and who can view your personal information, such as photos. Ensure that only friends have access to this information.
- Exercise caution when sharing photos or other content that may not be suitable for everyone.
- Exercise discretion when sharing information about others. Consider how your friends and family would feel if you shared their photos with strangers.
- Be mindful of your online persona as reflected in your social media posts and shares. Imagine that potential employers may scrutinize your online presence when evaluating you for a job.
- Exercise caution when engaging in online quizzes and contests. While they may seem entertaining, be aware that they collect information about you, including your interests, which can be sold to marketing companies with profit motives.
- When using a computing device that does not belong to you, opt for incognito browsing for enhanced security.
- When downloading applications, carefully evaluate whether they truly need access to your location, address book, photos, videos, etc., before granting such permissions.
- If you receive abusive images or messages at any time, take a screenshot of them and report the incident.

Global

Cyber Security Awareness Month in the USA

Cybersecurity Awareness Month is a collaboration between government and private industry to raise awareness about digital security and empower everyone to protect their personal data from digital forms of crime. The Cybersecurity and Infrastructure Agency (CISA) and the National Cybersecurity Alliance partner to create resources and communications for organizations to talk to their employees and customers about staying safe online.

While most of the cybersecurity news articles are about massive data breaches and hackers, it can seem overwhelming and feel like you're powerless against it. But Cybersecurity Awareness Month reminds everyone that there are all kinds of ways to keep your data protected. It can make a huge difference even by practicing the basics of cybersecurity.

- Cybersecurity Awareness Month 2023 will focus on four key behaviors all month long.
- Use strong passwords and a password manager.
- Turn on multifactor authentication.
- Recognize and report phishing.
- Update software.

Published By
CERT Media