ISSUE NO 02

Cyber Guardian

2024

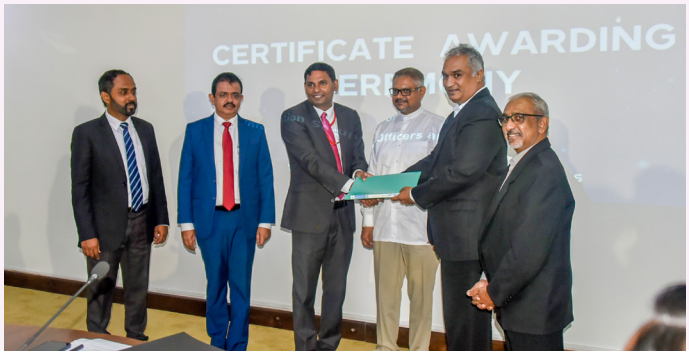
Publication for your online safety

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

Support the private sector in training government officials on cybersecurity

Sri Lanka CERT embarks on a groundbreaking journey with the Federation of Information Technology Industry Sri Lanka (FITIS) and the ISC2 Colombo Chapter, signing a momentous Memorandum of Understanding on April 3rd at SLIDA. This visionary collaboration sets the stage for mentoring and training 1,000 government officers over the next two years, elevating cybersecurity proficiency within government entities and the wider supply chain ecosystem.

In an ever-evolving digital landscape, collaboration emerges as the key to success. Through our partnership with the Federation of Information Technology Industry Sri Lanka (FITIS) and the ISC2 Colombo Chapter, we ignite a culture of innovation, knowledge exchange, and collective empowerment. This MoU underscores our commitment to advancing cybersecurity education, boosting awareness, and nurturing professional growth. Together, we empower government officials and supply chain stakeholders to navigate the complexities of the digital domain with confidence and resilience.
The distinguished guests present at the signing ceremony included Hon. Kanaka Herath, the State Minister of Technology, Dr. Dharmasri Kumarathunga, Secretary of the Ministry of Technology, Mr. Nalaka Kaluwewa, Director General of SLIDA, Mr. Andrew Shinn from the US Embassy of Sri Lanka, Mr. Janaka Sampath - Sri Lanka CERT Chairman (Actg) , CEO (Actg)Dr. Kanishka Karunasena, Mr. Indika De Zoysa, Chairman of FITIS and Mr. Sujit Christy, President of the ISC2 Colombo Chapter. Mr. Jayasiri Amarasena CEO of FITIS.



Policy//

Policy on Using Personal Devices for Official Work (4.3.22)

The organization shall not allow employees to use their personal laptops, smartphones and tabs to carry out official duties. However, under specific circumstances determined by the ISC, the organization may allow selected employees to use their personal devices to perform official duties, under the supervision of the ISO. In such circumstances, it is imperative to appropriately register such devices with the organization and ensure that those devices comply with this Policy.

However, Employees' personal devices shall not be used to process or store information classified as "Secret" and "Confidential" under any circumstance. When employees' personal devices are used to perform official duties, the organization shall ensure that user accounts are set up to have limited privileges, accounts are protected with strong passwords and multifactor authentication, antimalware software is installed and automatic updates are enabled, operating systems, utility software and other application software that is used have valid licenses with necessary patch updates.

Further, the organization reserves the right to review or retain personal and organizational information on such devices, or to release the information to government agencies or third parties during an investigation or legal requirement. Security of the personal device shall be the responsibility of the owner of the device.

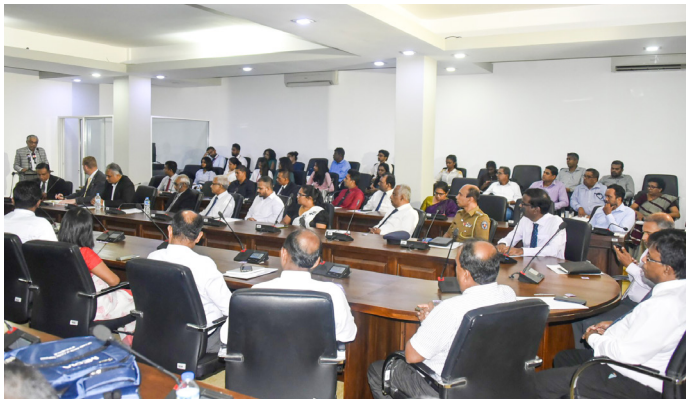
The organization shall not be liable for any loss or damage to the device including loss of personal data due to the use of the device.

Compliance: Applicable to all government organizations

Certificates were awarded to government officials and journalists who completed training in cyber security.

The officers who took part in the cyber security training course organized by the Sri Lanka CERT Institute for Chief Information Technology Officers, Assistant Information Technology Officers (ISO/ AISO) of Government Institutions were among the recipients. Recently, 60 officials from 37 government institutions attended the ceremony. Additionally, journalists were educated on cyber security and effective reporting of cyber security incidents to the public. Forty journalists who participated in this program will also receive certificates.

The certificate awarding ceremony took place at SLIDA, with Mr. Kanaka Herath, Minister of State for Technology, as the chief guest. Among the attendees were Dr. Dharmashree Kumaratunga, Secretary of the Ministry of Technology, Nalaka Kaluwewa, Director General of SLIDA, Andrew Shin from the US Embassy in Sri Lanka, Janaka Sampath, Acting Chairman of Sri Lanka CERT, Dr. Kanishka Karunasena, Acting CEO of Sri Lanka CERT, Indika de Soyza, President of FITIS, and Mr. Sujith Christie, President of ISC2 Colombo Chapter.



Is AI a Threat to Cybersecurity?

As consumers increasingly integrate AI tools into their daily lives, from managing meals to seeking medical advice, concerns about security and fraud risks arise. "**Info security Magazine"**'s findings, based on a KPMG survey report, highlight potential vulnerabilities even in well-implemented AI applications. Consumers willingly input sensitive information into these systems, potentially exposing themselves to harm. This not only jeopardizes individuals but also impacts businesses and overall cybersecurity protocols.

The survey indicates that a significant portion of consumers engage in risky behavior when using AI tools, often without considering the consequences. Over a third (38%) admit to inputting financial information, while 27% disclose personal details like addresses or dates of birth. Such data is invaluable to cybercriminals for identity theft, financial fraud, and other nefarious activities.

Moreover, 42% of individuals incorporate job-related information into AI tools for business purposes, risking the security of sensitive data. This underscores the potential for AI to become a threat to organizational security.

Cybercriminals are already leveraging scalable AI tools to enhance their attack methods. Consumer willingness to share confidential information exacerbates this threat. Coupled with emerging risks like deep fake AI impersonations, the digital landscape faces increased vulnerability to impostor attacks.

Despite a majority of users (59%) considering themselves knowledgeable about technology, many still fall prey to dangerous scams. Blaming consumers for such incidents has become commonplace, yet sectors like financial services (25%), healthcare (18%), and government (15%) advocate for stricter regulations. Approximately 20% believe all sectors should adhere to the same standards. However, consumers also bear responsibility in utilizing digital technologies with awareness to mitigate risks."