ISSUE NO 06

JANUARY 2024

Cyber Guardian

Publication for your online safety

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

World Bank facilitates Sri Lanka CERT to develop the National Cyber Security Strategy

Sri Lanka CERT with the support of the World Bank has made significant progress in developing the next version of the National Cyber Security Strategy (2024:2027). The primary objective of this strategy is to strengten the nation's cyber defences and resilience. During February, a series of stakeholder consultation sessions were conducted by Sri Lanka CERT with the active involvement of participants from various sectors including the public and private, academic, legal and policy, and civil societies. This inclusive approach ensures that the strategy reflects a broad spectrum of perspectives and priorities of cyber security.

The specific objectives aim to achieve through the implementation of the strategy include, (a) review and implement governance frameworks (b) establish policies for current and future technology (c) increase awareness (d) Enhance the expertise pipeline (e) strengthen incident response and recovery capabilities (f) Increase the technical capabilities of national cyber security operations (g) secure Critical Information Infrastructure (h) support broader stakeholder community (i) enhance international interaction and fulfill international obligations and (j) leverage local partnerships.

These objectives are classified into four Thrust Areas:

Thrust Area I- Enhance Legal and Regulatory Frameworks
Thrust Area II- Improve Knowledge
Thrust Area III- Strengthen Preparedness and Response Capacity
Thrust Area IV- Increase Cooperation

The next step of this strategy development activity is to submit the strategy for broader public consultation prior to obtaining the cabinet of ministers' approval. This transparent approach ensures that the National Cyber Security Strategy for Sri Lanka (2024-2027) reflects the needs, concerns, and aspirations of the entire nation.

Google deletes inactive accounts.

The process to deactivate all Google accounts that have been inactive for two years is set to begin. According to Google's policy, an account is considered inactive if there has been no login activity for two years. This criterion encompasses actions beyond just checking Gmail, including watching YouTube videos, performing Google searches, and downloading apps from the Play Store. Google had previously issued a warning in May of the last year regarding the upcoming deletion of such accounts. The underlying reason for this policy is the increased vulnerability of inactive

accounts to security breaches and their potential misuse in organized crime. Inactive accounts often rely on outdated or recycled passwords and lack two-factor authentication, making them easy targets. Ruth Critchley, Vice President at Google,has highlighted that accounts set up without proper security measures are particularly prone to exploitation by cybercriminals. This initiative is designed to 'safeguard personal information and prevent unauthorized account access, irrespective of whether the services are still in use.' Google has committed to providing users with at least eight months' notice before proceeding with account deletions. Once an account is deleted, its associated email address will be rendered unusable, thus securing old and potentially vulnerable addresses. According to 2022 data, daily Gmail activity is anticipated to exceed 121 billion

Make the Internet a safe place for your child:

1.Stay informed about your child's online and social media activities.
2.Remain cautious regarding friend requests, text messages, and emails from strangers.
3.Talk to your child about their friends on social media and teach them the significance of being selective about sharing photos and videos.
4.Familiarize yourself with your child's account usernames and passwords, and apply protective steps such as multifactor authentication.
5.Implement protective actions, like installing anti-virus software and using robust passwords, on every device connected to the Internet.
6.Instruct not to reveal passwords that are utilized for other online engagements, including educational platforms.
7.Educate not to publish any content that reveals your or your child's online identity on social media platforms and websites.
8.Instruct your children on the utilization of specialized applications endorsed by Internet service providers for improved cyber security.
9.Place the Internet-connected computer in a visible location. Set limits on online usage time and encourage engagement in other activities.
10. Promptly notify the appropriate authorities of any cases of Internet abuse.

KASPERSKY'S REGIONAL TEAM VISITS SRI LANKA CERT

On January 31st, the regional team from Kaspersky paid a visit to the Sri Lanka CERT. Among the representatives was Genie Gan Regional Director, Government Affairs & Public Policy, Siang Tiong- General Manager, South East Asia and Asia Emerging Countries, Lee Heng- Public Affairs Manager, APAC and Sam Yan- Head of Sales, Asia Emerging Countries from the Kaspersky team. The meeting served as a platform for discussions covering a range of topics.

During the visit, the Kaspersky team shared insights into the latest developments within their organization, including recent government partnerships, advancements in cyber security strategy development, and ongoing capacity building efforts. Furthermore, they elaborated on Kaspersky's involvement in national-level engagements in other countries.

The meeting marked a significant collaboration between Kaspersky and Sri Lanka CERT. Discussions indicated Kaspersky's willingness to extend support to Sri Lanka CERT in various areas, including sharing threat intelligence information, contributing to capacity building initiatives, and providing expert knowledge to aid in the development of strategies and policies.

This visit underscores the importance of collaboration between cybersecurity solutions & service providers and cyber security organizations in enhancing the nation's cyber resilience and preparedness.