ISSUE No 1

Cyber Guardian

Publication for your online safety

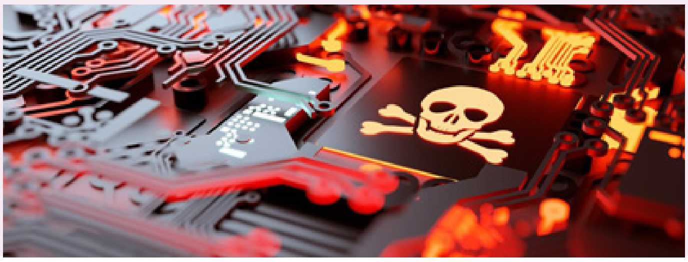
2024

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

Sri Lanka to Join US-led International Counter Ransomware Initiative

Sri Lanka has received an invitation to join the International Inaugural Action Against Ransomware, an initiative launched by the United States in 2021 alongside a coalition of other countries. This platform facilitates international coordination to combat ransomware.

To date, 48 countries, the European Union, and the International Police have become part of this initiative. Given Sri Lanka's recent challenges with ransomware attacks, it is believed that the country stands to gain significantly from participation in this global anti-ransomware effort.In response, the Cabinet of Ministers has endorsed a joint proposal by the Honorable President, in his dual roles as Minister of Technology and Minister of Justice, Prison Affairs, and Constitutional Reforms. This approval paves the way for Sri Lanka to join the International Initiative Against Ransomware and to take subsequent steps in this direction



Ensuring Your Security Identity's in the Digital Realm

How concerned are you about the security of your private network? Falling victim to a cybercriminal could lead to significant losses. This vulnerability opens the door for criminals to engage in activities such as stealing your bank funds or achieving other financial gains by using your identity for illicit purposes.
This includes applying for loans, acquiring fake identity cards, or obtaining identity documents using someone else's photo but your name. The consequences extend beyond financial loss; they subject you to considerable mental stress and demand significant effort to rectify.

Wondering how to tell if your identity has been stolen? Keep an eye out for unauthorized transactions or withdrawals in your bank statements, receipts for purchases you didn't make, statements for loans or credit cards you never applied for, unexpected notifications from government agencies, or rejections of loan applications due to fraudulent activities. These are telltale signs that your personal information may be at risk.

To protect yourself and your loved ones, consider the following precautions:

● Limit the personal information you share online. This includes refraining from posting photos or details that could reveal sensitive information, such as your address, children's school, or personal milestones, on social media.

● Adjust your social media privacy settings to 'Private' to control who can view your content. Share information only with people you trust and remain cautious about accepting friend requests from strangers.

● Stay vigilant against attempts by cybercriminals to trick you into divulging private information. They may impersonate reputable organizations through messages or counterfeit websites. Remember, genuine institutions typically do not solicit sensitive information through these channels, especially given the prevalence of fraud.

By adopting these strategies, you can enhance the security of your personal information and mitigate the risk of falling prey to cybercriminals.

The 'South Asia Regional Cybersecurity Conference' held in Sri Lanka

The "South Asia Regional Cyber security Conference,"organized by the CLDP program in collaboration with Sri Lanka CERT, marks a pivotal event designed to bolster regional cooperation in the realm of cybersecurity.

This conference draws participation from countries including the Maldives, Bangladesh, Nepal, India, and Sri Lanka, setting the stage for high-level speeches and key sessions dedicated to pinpointing areas that necessitate joint efforts to fortify cybersecurity measures. It aims to spark dialogue and foster collaboration among regional stakeholders—spanning government officials, industry experts, and academia—to tackle the emerging cybersecurity challenges facing the region.

The conference's agenda is packed with discussions on a variety of crucial cybersecurity themes, such as threat intelligence sharing, capacity building, incident response, and policy formulation. Through interactive sessions and workshops, attendees will seize the opportunity to exchange best practices, share knowledge, and uncover potential avenues for collaboration.

Ultimately, the conference seeks to cementregional partnerships and champion a unified approach to cybersecurity, thereby enhancing the digital safety and security of not only the participating nations but also the wider region.

Empowering Healthcare Guardians: Strengthening Cyber Hygiene

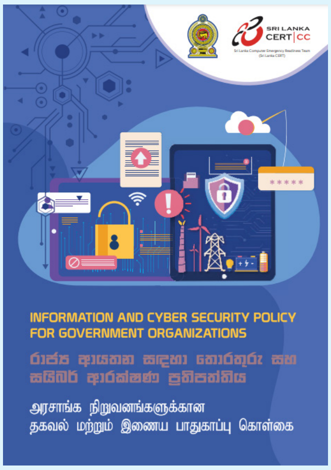
We are pleased to announce the successful completion of our recent Cyber Hygiene workshop, specifically designed for officials at the Ministry of Health.

In an era where digital advancements are revolutionizing healthcare, the imperative for robust cyber security measures cannot be overstated. Empowering healthcare providers with the necessary tools and knowledge not only protects data but also safeguards patient trust and confidentiality.

While not all participants may possess specialized expertise in cybersecurity, their roles are pivotal in maintaining the security and confidentiality of critical data. Our training was aimed at providing fundamental cyber security insights, implementing the Information and Cyber Security policy for government organizations, and introducing best practices tailored to the specific responsibilities within the healthcare sector.

The workshop attracted a diverse group of healthcare professionals from doctors to nurses, and focal points at district and provincial levels, representing the backbone of healthcare services across the country. With participants from every corner of the nation, the impact of this workshop resonates nationwide.

We extend our heartfelt thanks to all participants for their active engagement and commitment to enhancing cybersecurity practices within the healthcare sector. Together, we are forging a safer digital healthcare ecosystem.



SRI LANKA CERT|CC

INFORMATION AND CYBER SECURITY POLICY FOR GOVERNMENT ORGANIZATIONS

රාජ්‍ය ආයතන සඳහා තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

அரசாங்க நிறுவனங்களுக்கான
தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை

Policy on Using Non-Secure Networks

The staff of the organization shall avoid the use of non-secure networks, such as untrusted Wi-Fi networks (e.g. available in hotels, restaurants, bus stops), and the use of publicly shared personal computers, kiosks and other related devices to access official email and other official software solutions.

Compliance: Applicable to all government organizations