

CYBER GUARDIAN

Publication for your online safety

Sri Lanka CERT Urges Public to Remain Vigilant on Online Harassment and Scams.

The Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) has received more than 12650 complaints related to social media misuse and cybersecurity incidents in 2025. A significant proportion of the complaints involve fake account, hacked accounts and financial scams carried out through social media platforms.

Hateful or abusive content and adults' sexual harassments and content also feature high among the complaints said Charuka Damunupola the Lead Information Security Engineer of Sri Lanka CERT. He also said that there has also been an increase in general scams and the dissemination of false information, which affects both individuals and general public.



The cybercriminals continue to employ increasingly sophisticated and fraudulent methods to take advantage of the growing reliance on digital platforms for communication, trade, and financial activities. Particularly vulnerable groups, such as young people who might not be sufficiently informed of online safety procedures, elderly users, and first-time internet users, are frequently among the victims.

Charuka Damunupola, urges the public to remain vigilant, avoid sharing personal or financial information online, verify suspicious messages and links, and enable strong security measures such as two-factor authentication and secure passwords. In order to facilitate rapid response and mitigation, members of the public are also urged to promptly report cyber incidents to Sri Lanka CERT.

Sri Lanka CERT Hosts First Stakeholder Consultation on Ratification of UN Convention against Cybercrime

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), under the guidance of the Ministry of Digital Economy, convened its first stakeholder consultation session in December aimed at gathering expert insights and stakeholder perspectives on Sri Lanka's journey toward the ratification of the United Nations Convention against Cybercrime.

Mr. Varuna Sri Danapala Acting Secretary to the Ministry of Digital Economy chaired the stakeholder consultation attended by officials from the Ministry of Foreign Affairs, Ministry of Justice, Ministry of Public Security, Ministry of Defense, Attorney General's Department, National Child Protection Authority, CIABOC, and Sri Lanka Police.

At the beginning of the meeting Thilak Pathiraje the Chairman of Sri Lanka CERT welcomed the participants and Chamila Senanayake, Manager Legal and Regulatory Affairs of Sri Lanka CERT, drove the process leading to the signing of the UN Convention against Cybercrime and organized the stakeholder consultation.

Key technological and legal insights were presented by Senior Counsel Mr. Jayantha Fernando, who discussed the evolution of international legal frameworks on cybercrime and their impact on Sri Lanka's legal and regulatory landscape.

A comprehensive overview of the UN Convention against Cybercrime and how it might be integrated with Sri Lanka's current legal framework was provided by Mr. Sehan Soysa, Senior State Counsel of the Attorney General's Department at this session.



Four-Day Cybersecurity Audit Training for National Audit Office

The Sri Lanka Computer Emergency Readiness Team (CERT) conducted a four day training program for national audit officials of the National Audit Office on auditing cybersecurity initiatives in government organizations. The program aims to strengthen auditors'



capacity to assess cyber risk management, data protection, compliance, and governance frameworks within public institutions. With digital systems playing a growing role in government services, the initiative seeks to ensure strong oversight, accountability, and effective use of public funds allocated for cybersecurity.

Sri Lanka CERT Conducts Successful Cybersecurity Workshop for Media Professionals

The Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) successfully conducted a one day workshop titled "Encountering Cyber Threats in a Digital Era for Media Professionals" in December, at the SLIDA Auditorium, Colombo, with the participation of over 35 journalists representing print, electronic, and digital media institutions.

The workshop aimed to strengthen journalists' understanding of emerging cyber threats, digital safety, and responsible reporting in an increasingly complex digital environment. Participants engaged in interactive sessions covering cybercrime trends, online safety risks, misinformation, and the role of the media in cybersecurity awareness.

The event was graced by Mr. Waruna Sri Dhanapala, Acting Secretary to the Ministry of Digital Economy, who graced the occasion and awarded certificates to the participants. In his remarks, he highlighted the critical role of media professionals in promoting digital resilience and public awareness in Sri Lanka's digital transformation journey.

Sri Lanka CERT Warns Public of Rising Festive-Season & Disaster Related Social Media Scams



The Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) urges the public to remain extremely vigilant as a surge in online scams and embezzlement attempts has been observed across social media platforms in recent weeks.

These incidents coincide with the festive season and the ongoing climate related disaster situation, creating opportunities for cybercriminals to exploit public trust and vulnerability.

Sri Lanka CERT has received a significant number of complaints regarding fraudulent schemes where scammers impersonate government institutions, public service departments, reputed supermarkets, and well-known business entities. These actors circulate fake promotional offers, financial rewards, and prize announcements to mislead unsuspecting individuals.

In the aftermath of the recent cyclone and severe rains that caused widespread damage in several parts of the country, cybercriminals have also fraudulently replicated the names of government agencies and organizations involved in relief and recovery efforts. They distribute deceptive links and persuade the public to donate money through these channels, resulting in many victims losing funds directly from their bank accounts.

Sri Lanka CERT strongly reminds the public not to click on suspicious links, not to share personal information, and never to disclose banking details or One-Time Passwords (OTPs) with unknown individuals or unverified websites.



report@cert.gov.lk



www.cert.gov.lk
www.onlinesafety.lk