सीएसआईआर
CSIR
भारत का नवाचार इंजन
The Innovation Engine of India

CSIR CYBER SECURITY AWARENESS

Beware and Stay Safe from **Cyber Attacks**

Internet Browsing and Email Security

Internet browsing security involves protecting online activities from cyber threats like phishing, malware, and unauthorized access. It includes using updated browsers, enabling security features, and avoiding suspicious websites and links.

Email security focuses on safeguarding email communications from threats such as phishing, malware, and unauthorized access. It involves using strong passwords, and being cautious about opening suspicious emails or attachments.

Do’s

- Use Private/Incognito Mode for government, email, banking, or sensitive services.
- Manually type the URL/domain name instead of clicking on links.
- Use the latest version of browsers and keep them updated.
- Configure Kavach Multi-Factor Authentication on NIC email accounts.
- Download the Kavach app only from valid app stores.
- Regularly review NIC email login history and report any discrepancies.
- Use PGP or digital certificates to encrypt important emails.

Don’ts

- Avoid storing payment details in the browser.
- Do not use 3rd-party anonymization services like VPNs, Tor, or proxies.
- Never download unauthorized or pirated content from the internet. Do not open links or attachments from unknown senders.
- Do not use official systems for installing or playing games.
- Be cautious with shortened URLs, as they may lead to phishing or malware sites.
- Do not share email passwords or Kavach OTPs with unauthorized persons.
- Avoid using external/unauthorized email services for official communication.

FOR REPORTING SECURITY INCIDENTS: incident@csir.res.in