CSIR CYBER SECURITY AWARENESS

Beware and Stay Safe from Cyber Attacks

Social Media Security

Social media security focuses on protecting personal and organizational information shared on social platforms from threats like phishing, identity theft, and unauthorized access. It involves enabling strong authentication, being cautious with sharing sensitive data, avoiding suspicious links, and regularly reviewing account privacy settings to prevent misuse or cyberattacks.

Do's

- Limit sharing of personal information on social media.
- Verify a contact's authenticity before accepting friend requests.
- Enable Multi-Factor Authentication for account security.
- Regularly review and update privacy settings to control who can view your content.
- Enable account activity alerts to monitor unauthorized access.
- Use secure, trusted apps for social media management.
- Log out from accounts when using shared or public devices.

Don'ts

- Do not click on links or files from unknown contacts/users.
- Avoid sharing internal government documents on social media.
- Do not post unverified information on social platforms.
- Never share your @gov.in/@nic.in email address on social media.
- Avoid using third-party apps; prefer NIC's Sandes App for official communication.
- Avoid using public Wi-Fi when accessing social media accounts.
- Do not download apps or content from untrusted sources linked through social media.

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