CSIR CYBER SECURITY AWARENESS

Beware and Stay Safe from SPEAR PHISHING ATTACKS

Spear Phishing is a type of phishing attack, where the attacker targets a specific or a group of individuals or a Department, with customized phishing content tailor made to compromise the target.

COMMON TRAITS OF SPEAR PHISHING MAILS TARGETED AT CSIR EMPLOYEES

01 The Sender & Recipient of the Phishing Mail would be the same Email Address. You will be in Bcc

02 Use of Shortened URLs for links (ex: https://tinyurl.cc/aJkm3)

03 Use of Subject like : Conference/Lecture Invite, Research Paper, Foreign Visit, DA Hike, Arrears, Pay Fixation, Tender, Bill Payment, Meeting Request, VPN, Email Migration….etc

04 Mails with Password Protected Attachments, where password is shared in the Mail body

05 Mails advising you to download an Application / Software hosted on external links (i.e., other than "*.csir.res.in" or "*.gov.in" or "*.nic.in" sites) for accessing a CSIR or Govt Application / Service

WHAT TO DO IF YOU RECEIVE A PHISHING/SUSPICIOUS MAIL

- Don't Click on the URLs /Links present in the Mail
- Don't open the attachments present in the Mail
- Don't respond to the Mail
- Don't Upload or share the contents of the Mail with any external/3rd party sites or Apps
- Report the mail to incident@csir.res.in

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