NLC India Limited
(**"Navratna"** – A Government of India Enterprise)

Office of the Chief General Manager / Computer Services & ERP
Corporate Office
Telephone No.04142-212348 Fax No. 04142 - 252645 /252646

CIRCULAR

Cir No. CGM/CS/CybSecy/2024-10 Dt: 30.10.2024

Sub : Advisory on phishing mails– Reg
Ref: NIC-CISG/2024-10/546 dtd 17.10.2024

1. Employees are hereby requested to take extreme precautions while processing emails considering the recent escalation in cyber-attacks using phishing mails. Phishing emails typically aim to trick recipients into clicking on malicious links or attachments, leading to data theft, malware infection, unauthorized access to accounts. It is a fraudulent attempt to obtain sensitive information (such as usernames, passwords, credit card numbers, or other personal details) by masquerading as a trustworthy web site.

2. An advisory issued vide ref. above by National Informatics Center (NIC), in this regard is attached as Annexure

3. Phishing emails can be recognized with the following characteristics.

   i. Mails received from unknown sources must be treated with utmost precaution. They appear to come from a domain imitating legitimate domains.

   ii. Urgency in the request to click the URL, warning of account suspension, unauthorized access, or immediate action needed to avoid a penalty.

   iii. Spelling or grammatical mistakes e.g. nlcindia.in where the first "i" may be replaced by "l", or gov.in, where the "o" may be replaced by a "0" (zero).

   iv. Request to share credentials , passwords and sensitive information including credit card nos etc.,

   v. Images of text used in place of normal text to prompt user action by clicking the image

   vi. Usage of Bit.Ly or other link shortening techniques.

4. In case, the phishing URL is already clicked, the following may be carried out.

   i. Suspicious message must be immediately reported to unit CS nodal officer

   ii. The phishing mails may be deleted.

   iii. The endpoint must be immediately disconnected from network

   iv. The passwords of the affected endpoint may be changed.

   v. Complete anti-virus scan may be run and files may be backed up to an external hard drive .

vi. Ensure Operating System, Web Browsers, and other Software are updated with the latest security patches.

By following above steps, the potential risks associated with clicking on a phishing URL may be mitigated.

5. Recently attackers posing as IT support staff from Microsoft Teams sent spam emails from impersonated accounts which seemed to appear legitimate, using names like "securityadminhelper" or "supportserviceadmin,". If links in such emails are clicked, the attackers gain access to install malicious tools, move laterally across the network, steal data, and ultimately deploy malware. As this attack is through trusted platforms like Microsoft Teams, employees are advised to remain extra vigilant in such cases, refrain from clicking links and report the same to unit CS nodal officers.

Solomon 30/10/24
CGM/CCS&ERP

Copy
To All Executive Directors
All Heads of Units/Projects/JVs/Offices
All Group Heads of HR/Finance
All Unit HoHRs & Finance Heads
All Account Centers
Copy to:
TS/PS to CVO/FDs/CMD