No. AV-29016/3/2025-Cyber Security Cell-MoCA
Government of India
Ministry of Civil Aviation
*****

Block B, Rajiv Gandhi Bhawan,
New Delhi, Dated the 08th April, 2025

To,

1. All Division/Section, MoCA
2. All attached offices, MoCA

Subject: Circulation of advisory regarding Phishing

Sir/Madam,

Please find attached herewith a copy of the advisory dated 19.03.2025 received from the Cyber & Information Security Group, NIC regarding the above subject, vide which several recommendations were outlined for identifying and mitigating phishing attacks. Further, it is recommended that this advisory be circulated to all officials of the ministry/department.

2. It is requested to share this advisory among all officials and encourage adherence to the outlined mitigation measures.

Yours faithfully,

(Kumar Saurabh Raj)
Director
Tel: 011-24653565

Enclosure: As above

Copy to: SDIT Division, MoCA – For publishing the same on Notice board, eOffice

CIS Governance Division
Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2025-03/055
Dated: 19-03-2025

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Advisory for Phishing

Description:

Phishing is a type of cyberattack where scammers impersonate trusted sources to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal details. These attacks often come through emails, messages, or fake websites designed to look legitimate.

In view of above, NIC-Cyber Security Group advises following:

1. In case a phishing mail is received, do not enter your NIC Login Credentials when redirected login prompt appears.
2. Delete phishing emails from your inbox.
3. In case, you have already clicked a phishing URL
   a. Take your device offline – Disable your internet connection.
   b. Change your password - You need to change the passwords for any accounts that might have been hit in the cyberattack.
   c. Change your passwords from a different device to ensure that the hacker can't access your new information.
   d. Turn on multi-factor authentication for the account that might have been attacked.
   e. Back up your files - To protect your data from the phishing attack, back up your files to an external hard drive or USB.
   f. Scan your device with anti-virus software.
   g. Update your Operating System, Web Browsers, and other Software with the latest security patches.
   h. Report suspicious message to your email service provider or NIC designated mail address
   i. Avoid sharing personal information.

By following above steps, you can effectively sanitize your system and mitigate the potential risks associated with clicking on a phishing URL.

Some ways to recognise a phishing email are given below:

a. Be suspicious of emails that claim you must click, call, or open an attachment immediately or urgently.
b. If a mail received from unknown source, this may be a source of phishing.
c. If an email message has obvious spelling or grammatical errors, it might be a scam. e.g. nlc.in where the first "i" has been replaced by "l", or gov.in, where the "o" has been replaced by a "0" (zero).
d. Images of text used in place of text (in messages or on linked web pages) may be scam.
e. Be cautious of links shortened by using Bit.Ly or other link shortening techniques.