
	<p>रक्षा लेखा प्रधान नियंत्रक (मध्यकमान) 1 करियप्पा मार्ग, लखनऊ छावनी-226002 Principal Controller of Defence Accounts (Central Command) 1 Cariappa Road, Lucknow Cantt.- 226002 कार्यालय फोन सं.-0522-2451084/कार्यालय फ़ैक्स सं-0522-2453038 Office Phone No.-0522-2451084/Office Fax No.-0522-2453038 E.Mail- <a href="mailto:cda-luck@nic.in">cda-luck@nic.in</a> &amp; <a href="mailto:pcdacedp.dad@gov.in">pcdacedp.dad@gov.in</a></p>	 आज़ादी अमृत महोत्सव
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------

Circular

No. IT&S/AN/174/Cyber Security/2023-24

Date: 17/07/2023

To,  
The Officer-in-Charge  
All sections of Main Office  
All sub-offices  
Under PCDA (CC) Lucknow

**Sub:- Advisory – Phishing email within MoD.**

**Ref:- HQrs office circular no Mech/IT&S/810/Cyber Security dated 17/07/2023.**

With reference to HQrs office circular cited under reference, an advisory is issued regarding “Phishing email within MoD”. A copy of the same is enclosed herewith for your information & to disseminate the guidelines to all concerned for strict compliance.

It is also requested to submit an action taken report to this office latest by 20/07/2023 at 03:00PM.

Encl: As above.

  
Sr. Accounts Officer (IT&S)

Copy to:

OA Cell (Local): for uploading on website.

  
Sr. Accounts Officer (IT&S)

“ हर काम देश के नाम ”

## रक्षा लेखा महानियंत्रक

उलान बटारोड, पालम, दिल्ली छावनी-110010



Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt.- 110010

(IT&S Wing)

Phone: 011-25665586, 2566589, 25665763 Fax: 011-25675030 email:cgdarnewdelhi@nic.in

No: Mech/ IT&S/810/Cyber Security

**Circular**

Date: 17/07/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)  
(through DAD WAN)

**Sub: Advisory - Phishing email within MoD.**

In the wake of recent spate of phishing emails being received within the email IDs, it is advised to all the personnel to be aware of phishing mails and how to prevent cyber incidents due to it.

2. In continuation of all the advisories disseminated earlier, a list of cyber security best practices is mentioned below:

### Do's :

- **Be cautious and skeptical:** Always approach emails with caution, especially those from unknown or suspicious sources.
- **Verify the sender:** check the sender's email address and ensure it matches the official contact information of the organization they claim to represent.
- **Check for spelling and grammar errors:** Phishing emails often contain typos, grammatical mistakes or awkward language.
- **Hover before you click:** Hover your mouse over any links in the email to reveal the actual URL. Ensure the URL matches the one displayed in the email and is not a deceptive link.
- **Keep software up to date:** Regularly update your email client, web browser and operating system to protect against known vulnerabilities.
- **Use strong, unique passwords:** Create strong passwords and use a password manager to securely store them.
- **Enable two factor authentication (2FA):** Enable 2FA whenever possible to provide an extra layer of security for your email account.
- **Educate yourself:** Stay informed about the latest phishing and scams to better recognize and avoid them.

### Don'ts :

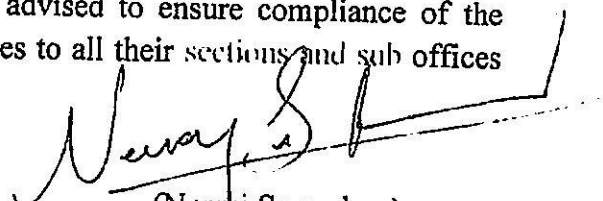
- **Don't click on suspicious links:** Avoid clicking on links in emails unless you are confident about their authenticity.
- **Don't download attachments from unknown sources:** Be cautious when downloading attachments, especially if they are unexpected or from unfamiliar senders.

- **Don't provide personal information:** Legitimate organizations would never ask for personal or financial information via email. Avoid sharing sensitive data like passwords, credit card details, or social security numbers through email.
- **Don't trust urgent or threatening messages:** Phishing emails often use urgent or threatening language to manipulate victims. Be skeptical of such messages and verify their legitimacy through other means.

**Cyber Hygiene Steps:**

- **Use robust email filters:** Enable strong spam filters and configure them to mark or divert suspicious emails to spam folder.
- **Install antivirus and anti-malware software:** Keep your computer protected with up-to-date security software to detect and block phishing attempts.
- **Regularly back up your data:** Create regular backups of important files and data to mitigate the impact of any potential phishing attacks.
- **Report phishing attempts:** If you receive a phishing email, report it to your email provider and relevant authorities so that appropriate action can be taken.
- **Stay updated on security best practices:** Continuously educate yourself about cybersecurity best practices and follow the latest recommendations to enhance your online security.

3. In view of the above, all the Controllers are advised to ensure compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance.



(Neeraj Surendran)  
Sr. ACGDA (IT&S)