

I/11489/2023



रक्षा लेखा नियंत्रक (सेना)

Controller of Defence Accounts(Army)

बेल्चेडियर परिसर, आयुध पथ, मेरठ छावनी- 250001

Belvedere Complex, Ayudh Path, Meerut Cantt-250001

**Through Website**

No. IT&S/III/Cyber Security/2023

Date: 28/07/2023

To

All sections of Main Office**All sub-offices of CDA (Army) Meerut****Sub:** Advisory - Phishing Email within MoD.

"Phishing" is the practice of sending fraudulent communication that appear to originate from a reputable/trustworthy source. It is a common type of cyber attack and is usually done through email. The goal is to steal sensitive financial and login information, or to install malware on the victim's computer.

In view of the above, a copy of HQrs Office letter No. Mech/IT&S/810/Cyber Security dated 17.07.2023 which is an advisory to avert any phishing-related cyber incidents and to sensitize all employees towards better cyber practices is forwarded herewith for strict compliance.

This issues with the approval of GO (IT&S).

Encl: As stated above.

NAVEEN PRAKASH, AO(IT&S)-NAVEENP, IT&S-ARMY
Accounts Officer

“ हर काम देश के नाम ”

रक्षा लेखा महानियंत्रक

उलान बटाररोड, पालम, दिल्ली छावनी-110010



Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt - 110010

(IT&S Wing)

Phone: 011 25665586, 25665589, 25665763 Fax: 011 25675030 email:cgdanewdelhi@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)

Handwritten signature and initials in green ink.

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 :

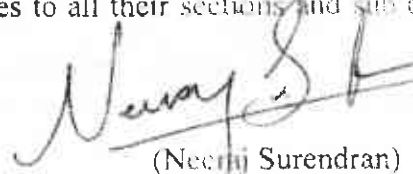
- **Don't click on suspicious links:** Avoid clicking on links in emails unless you are confident about their authenticity.
- **Don't download attachments from unknown sources:** Be cautious when downloading attachments, especially if they are unexpected or from unfamiliar senders.

- **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 Controllors 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)