
	<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- cda-luck@nic.in & pcdacedp.dad@gov.in</p>	 <p>आजादी का अमृत महोत्सव</p>
---	---	--

Circular

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

Date: 7/07/2023

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

Sub:- Advisory – Phishing Campaign by Cyber Threat actors.

Ref:- HQrs office circular no Mech/IT&S/810/Cyber Security dated 12/07/2023.

With reference to HQrs office circular cited under reference, an advisory is issued regarding “Phishing Campaign by Cyber Threat actors”. 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.

Copy to:

OA Cell (Local): for uploading on website.


Sr. Accounts Officer (IT&S)


Sr. Accounts Officer (IT&S)

“ 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)

cgdanewdelhi@nic.in

No. Moch/ IT&S/810/Cyber Security

Circular

Date: 12/07/2023

To,

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)

Sub: Advisory - Phishing Campaign by Cyber Threat actors .

Recently it has come to notice that a phishing URL 'https://drdo.gov.in.cyberdefenceexercise.cyou/cyberdefenceexercise.html' mimicking website of DRDO is in mass circulation since 03rd June 2023 within various sensitive government organisations including Defence establishments to harvest the NIC credentials of government officials under the pretext of Defence Cyber Exercise (DCX) through a compromised NIC email ID "mkjaiswal@ord.gov.in".

2. Additionally, some more such phishing campaigns are actively pursuing credential harvesting of Defence personnel under various pretexts which are shown in the table below:

S. No	Malicious Domain	IP Address
a.	cyberdefenceexercise.cyou	185.20.187.75 185.20.184.6 198.54.16.98
b.	aiapplication.chat	68.65.121.178
c.	vigilancedep.info	104.21.34.145
d.	kavachmail.in	104.21.64.80
e.	mod-info.xyz	68.65.121.153

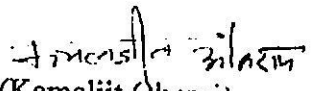
3. The following compromised NIC email IDs were used to originate phishing campaigns:

S. No	Compromised email-ID
a.	manas.230192-cgo@gov.in
b.	coladm.afmc@nic.in
c.	msslakshmi.debel@gov.in
d.	jsns@dddpmo.gov.in
e.	Project75@navy.gov.in
f.	xanthopsia@nic.in

g.	olsbag@iaf.nic.in
h.	sao.33wg@iaf.nic.in
i.	devendra.k13@nic.in
j.	mkjaiswal@ord.gov.in
k.	captmaheshcmoudgil@gmail.com

4. In view of the above, the following actions are to be taken to contain spread of these campaigns:
- Block the suspicious URLs and the IPs mentioned in the table at para 2 at perimeter security devices.
 - Sensitize all personnel under respective AOR regarding these phishing campaigns along with the modus operandi and advise them not to enter their NIC login credentials when redirected login page appears. Users to be also advised that any e-mail received from compromised IDs at para 3 above should not be opened.
 - Forward any suspicious emails to DCyA email ID (soc.ids@gov.in) without clicking on any link/opening any attachments/enter credentials for analysis and further guidelines.
 - Post forwarding to DCyA, delete phishing emails from the inbox and trash folders of all the recipients.
5. In view of the above, all the Controllers are advised to ensure strict compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance. Action taken report may please be forwarded to this office at the earliest.

Jt. CGDA (IT&S) has seen.


(Kamaljit Oberoi)
SAO (IT&S)