



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

75
आज़ादी का
अमृत महोत्सव

Important Circular

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

Dated 06/09/2023

To

The Officer-in-Charge

All sections of Main Office

All Sub Offices under PCDA(CC)

Sub: Guidelines regarding Domains registered by Pak Malicious Actors.

Ref: CGDA Hqrs office circular No.Mech/IT&S/810/Cyber Security/Misc dated 04-09-2023 (copy enclosed).

As conveyed vide CGDA HQrs office circular cited above, it is brought to notice that few websites have been registered under ".in" domain which are originally hosted by Pak based malicious actors. These websites are hosted to trap Indian Defence Personnel. List of such identified websites and immediate actions to be taken in this regard has been communicated through the circular.

Kindly go through the content of the circular and ensure necessary actions accordingly. A compliance report in this regard may please be emailed to pcdacedp.dad@gov.in by 10 AM on 08-09-2023.

Encls.-As above

sd

Sr.A.O.(IT&S)

Copy to-

OA Cell(Local)

For uploading on website.

पुनर्
Sr.A.O.(IT&S)

रक्षा लेखा महानियंत्रक

उत्तान बटारोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts
Ulan Batar Road, Palam, Delhi Cantt. 110010
(IT & S-Wing)

Phone: 011-2612588 Fax: 011-2612587 Email: gclanewdelhi@nic.in

Mech IT&S/810/Cyber Security/Misc Circular

Date: 04/09/2023

To:

All PCsDA, CsDA, PrIFA, IFA, PC, AFys
(through DAD WAN email)

Subj: Domains registered by Pak Malicious Actors.

It has been observed that few websites have been registered under ".in" domain which are originally hosted by Pak based malicious actors. These websites are hosted to trap Indian Defence Personnel. The list of websites identified till date are as under :

S. No	Malicious Domain
a.	coorddesk.in
b.	ksboards.in
c.	dopt.ecordsec.in
d.	ksb.esl.in
e.	esb.esl.in
f.	cgda.esl.in
g.	adminbr.in
h.	coordbranch.in
i.	coordbr.in
j.	e-admin.in
k.	admndesk.in
l.	ksbpanel.in

Handwritten notes:
SMD (IT/S)
KMD
Perf up complete report by 08/9/23
08/9/23

Handwritten notes:
S. S.P. Singh, AAO
for n.a. pl
09/9/23

938
IT/S

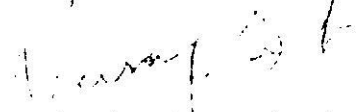
2. Further research at national levels is in progress to identify more such domains. These domains can be used to launch spear phishing attacks against Armed forces.

3. In view of the above, the following actions are to be taken immediately to contain spread of these campaigns:

- Block the malicious URLs mentioned at para 2 above at perimeter security devices of AF IISOs.
- Sensitise all personnel under respective AOR regarding these phishing campaigns originating from these phishing domains and download applications only from trusted websites.
- Sensitise persons to not enter their NIC login credentials when redirected login page appears.

- Forward any suspicious emails DCyA email ID (soc.adsa@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.

4. 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)