भारत सरकार, रक्षा मंत्रालय
Govt. of India, Ministry of Defence,
कार्यालय रक्षा लेखा प्रधान नियंत्रक (प.क.)
Principal Controller of Defence Accounts (WC),
चडीगढ़ 160022, दूरभाष सं० 0172-2741612
Chandigarh -160022,Phone No. 0172-2741612
Email-cda-chd@nic.in

सत्यमेव जयते

THROUGH WEBSITE

No. IT&S/Cell/1354/Cyber Security/2023

Date:12-09-2023

Circular

To
The Officer-in-Charge
All Sections of Main Office
All Sub Offices under PCDA(WC) Chandigarh

Sub:- **Advisories regarding Domains registered by Pak Malicious Actors and SOP for MoD Net/Internet Users.**

Ref:- 02 HQrs office **Circular letter No- Mech/IT&S/810/Cyber Security/Misc, dated-** 04/09/2023.

02 HQrs Office letters cited under reference are being forwarded herewith to all concerned for strict compliance regarding Domains registered by Pak Malicious Actors and Standard Operating Procedure (SOP) for MoD Net/Internet Users to mitigate issues related to Cyber and Phishing attacks.

GO(IT&S) has seen.

Encls: As above.

Sr.AO(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)

Phone: 011-25665588 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security/Misc **Circular** Date: 04/09/2023

To

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

Sub: 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.ccordsec.in
d.	ksb.cs1.in
e.	rsb.cs1.in
f.	cgda.cs1.in
g.	adminbr.in
h.	coordbranch.in
i.	coordbr.in
j.	e-admin.in
k.	admindesk.in
l.	ksbpanel.in

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 AFTI/JSOs.
- 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.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.

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)

“ 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: 011-25665588 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security/Misc **Circular** Date: 04/09/2023

To

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

Sub: Standard Operating Procedure (SOP) for MoD Net/Internet Users.

In view of the increasing number of cyber threats and compromise incidents, a Standard Operating Procedure (SOP) for endpoint users is circulated by MoD :

➤ **Standard Operating Procedure (SOP) for MoDNet/Internet users :**

a) It is mandated to use any hardened Linux or Maya-OS along with chakra agent, in all the internet facing endpoints/PCs of MoD.

b) No data processing or transmission of classified data, confidential and above, should be done on Internet endpoints/PCs, separate non Internet connected work PCs to be used by all departments.

c) All the officials/staff while receiving mail with attachments should due diligently cross verify the credentials of the sender before downloading the attachment/clicking on any link.

d) In case any call is received pertaining to any mail attachment or password thereof, the credibility of the caller should be ascertained by giving a call back to the calling number. Only landline numbers should be accepted for such verification.

e) MoDNet Intranet (Air gapped network) to be used for data transmission/official work in DoD, DDP, DESW and MoD Fin.

f) Usage of smartphones to be restricted and non approved officials/staff should not be allowed access of smartphone at workplace.

g) Ensure that no internet dongles/Mobile devices/WiFi/USB storage devices are plugged into Intranet (Air gapped, Network) systems/MoDNet.

h) MeitY guidelines on the usage of Operating system to be followed in respect of standalone/intranet PCs/System. It should be ensured that operating systems are kept up to date with the latest authentic patch releases.

2. All the Controllers are advised to ensure compliance of the SOP given above and disseminate these to all the officials of their sections and sub offices for strict compliance.

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