"हिंदी भाषा राष्ट्र निर्माण में सहायक है"

रक्षा लेखा प्रधान नियंत्रक) मध्य कमान (1 करियप्पा मार्ग, लखनऊ छावनी226002-
Principal Controller of Defence Accounts (Central Command) 1 Cariappa Road, Lucknow Cantt.– 226002
कार्यालय फोन सं2453038-0522-कार्यालय फ़ैक्स सं/2451084-0522-.
Office Phone No.-0522-2451084/Office Fax No.-0522-2453038
E.Mail- cda-luck@nic.in

IMPORTANT CIRCULAR

No: EDP/AN/174/Cyber Security/2022-23 Date: 09 /12/2022

To,

Officer-in-Charge
All Sub-Offices (Under PCDA (CC))
All Sections (Local)

Sub : Advisory regarding prevention of data breach.
Ref : HQrs Letter No. Mech/IT&S/810/Cyber Security dated 06.12.2022 .

****

A copy of CGDA HQrs office letter cited under reference regarding Prevention of data breach is enclosed with this letter. Instructions contained therein are to be strictly complied with by all offices and sections under PCDA (CC).

A rise in incidents of data breach and data leaks have been continuously observed in the official environment. Please ensure strict compliance of the guidelines issued by the HQrs office vide letter no. cited above.

Sr. Accounts Officer
(IT&S)

Copy to:
The officer-in-charge
OA Cell
(Local)
} For uploading on website.

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
Phone: 011-25665586, 25665589, 25665763 Fax: 011-25675030email:cgdanewdelhi@nic.in

E-mail

CIRCULAR

No. Mech/ IT&S/810/Cyber Security Date: 06/12/2022

To

All PCsDA/CsDA/PCA(Fys)/Pr.IFA/IFA

Sub: Advisory regarding prevention of data breach.

A rise in incidents of data breach and data leaks affecting data/ PCs and emails is being continuously observed in the official environment. Attackers use a variety of techniques to gain access to the internal networks,servers and databases. Also, attackers exfiltrate data and then deploy ransom ware to encrypt the data they have stolen and release the stolen data in public domain.

2. In this regard, CERT-In has issued an Advisory targeting the prevention practices of the data breach.

3. In view of the above, the following instructions mentioned in the CERT-In Advisory letter may please be circulated in all the sections/sub offices under your organization for strict compliance by all. The instructions for compliance are as follows:

a) Usage of strong and unique passwords for all the online accounts. Use different passwords for different online accounts. Enable two-factor authentication wherever available.

b) Regularly update all the software on computers and other devices. Install a reputed anti-virus solution on systems, keep it updated and configure it to run scans periodically.

c) Be wary of clicking links received in unsolicited SMS messages or emails. Do not open email attachments from unknown senders. Limit sharing personal information on public online forums.

d) While making online payments, ensure that the merchant website as well as the payment gateway websites are running on HTTPS and have a valid certificate (usually shown as a "green lock" symbol near the address bar in most browsers).

e) Do not share personal information, OTPs etc. over phone calls purporting to come from customer service, bank etc. Refuse to install any apps on smartphone / computer if asked to do so by an unknown person over phone call or in person.

f) It is advised to use Linux on internet connected PCs.

g) Employees must be advised to avoid mixing personal with work email and/or work documents, or allowing someone they shouldn't , to use their official device or sharing official information with them.

h) Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest.

i) Develop and maintain strong policies enforcing strong passwords (password management) .

4. In continuation to the above, the followings steps should be followed for prevention in email data breaches:

i. The user needs to change the password from a computer which is Virus/malware free.

ii. Get the machine scanned with latest patches of Anti Virus on which one is accessing the mail and also get their OS updated with the latest patches.

iii. Check whether any key logger is present in the system.

iv. The users need to ensure that the "REMEMBER PASSWORD" option isn't configured anywhere i.e. in the browser or in POP client i.e. outlook, thunder bird etc.

5. All Controllers are advised to ensure strict compliance of the guidelines given above. Action taken report may please be forwarded to HQrs office .

Jt. CGDA (IT&S) has seen.

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