कार्यालयरक्षालेखाप्रधाननियंत्रक
सं. 107, लोअरअग्रमरोड, अग्रमपोस्ट, बेंगलूर- 560 007
Office of the Principal Controller of Defence Accounts
No. 107, Lower Agram Road, Agram Post, Bangalore – 560 007
फोननं./Phone No. - 29710474/75फैक्सनं. /Fax No. - 26710132/33
e-mail: cda-blor@hub.nic.in

No. EDP/Mech/Gen. Corr Dated: 30-06-2023

CIRCULAR

To,
All IDAS
All SAOs/AOs
All the Sections in the Main Office
All the Sub-Offices under the O/o PCDA Bangalore

Sub: Cyber Security Advisories - regarding.
Ref: HQRs Circular Letter No. Mech/IT&S/810/Cyber Security Dated 22-06-2023

HQRs Office has been circulating advisories from time to time to all the controllers regarding Cyber hygiene and to mitigate issues related to Brower attacks for NIC email accounts.

In this regard, it is reiterated to strictly follow the guidelines given below:

A. Cyber Security Guidelines for employees from Govt. of India:

a. Desktop and printer security at the office:
   i. Set up unique passcodes for shared printers.
   ii. Always lock/log off from the desktop when not in use or before leaving the office.
   iii. Enable desktop firewall for controlling information access.
   iv. Ensure that the antivirus client installed on your systems is updated with the latest virus definitions, signatures and patches.
   v. Ensure that the Operating system and BIOS firmware are updated and set BIOS password for booting.
   vi. GPS, Bluetooth, NFC and other sensors on the desktop should only be enabled when required.
   vii. Use of all pirated Operating systems and applications should be deleted.

b. Password Management:
   i. Use multi-factor password authentication.
   ii. Use complex passwords and change passwords at least once in 30 days.
   iii. Don't save passwords in the browser and don't use the same password on multiple websites/apps.

c. Internet Browsing Security:
   i. Any third-party anonymization services and toolbars are prohibited in the office's internet browser.
   ii. Don't use Incognito mode while accessing govt. applications, email services or payment-related services.
   iii. Don't download any unauthorized or pirated content/software from the internet.
   iv. Don't store any usernames, passwords and payment-related information on the internet browser.
   v. Always type the site's domain name/URL manually on the browser's address bar while accessing sites where user login is required, rather than clicking on any link.

d. Email Security:
   i. Ensure that Kavach multi-factor authentication is configured on the NIC email account.
   ii. Regularly review the past login activities on NIC's email service by clicking on the "login history" tab. If any discrepancy is observed in the login history, the same should be immediately reported to NIC-CERT.
   iii. Don't click any link or attachment contained in emails sent by an unknown sender.

e. Removable Media Security:
   i. Don't plug-in the removable media on any unauthorized devices.
   ii. Scan the removable media with Antivirus software before accessing it and perform a secure wipe to delete the contents of the removable media.

f. Security Advisory and Incident Reporting:
   i. Adhere to Security advisories published by NIC-CERT (https://niccert.nic.in) and CERT-In(https://cert-in.org.in)
   ii. Report any cyber security incident, including suspicious mails and phishing mails to NIC-CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in)

B. Cyber Security Measures- Dark Web usage:

a. Avoid visiting/browsing Dark and Deep web.
b. Inform authorities in case of any compromise or honey trap through the usage of Darkweb.

C. Vulnerability in Kavach Authenticator:

a. Kavach Authenticator to be logged in for use on daily basis and be logged out after OTP generation.
b. Don't use 'keep logged in' options in Kavach Authenticator and NIC e-mail on any devices.