कार्यालय रक्षा लेखा नियंत्रक (सेना), मेरठ छावनी
Office of CDA (Army)

बेलवेडीयर परिसर, आयुध पथ, मेरठ छावनी

Belvedere Complex, Ayudh Path, Meerut Cantt-250001

फोन:0121-2646632 फैक्स नंबर :0121-2646254, 2646216

No. AN/II/Disc/EK/I Dated: 16.12.2022

CIRCULAR

To,

1. All GOs/SAOs/AOs
2. Offices incharge,
   All sections, Main Office.
3. Officers incharge
   All sub-offices

Subject : Strict Compliance of recommendations issued by CIRA (Cyber Information Research Agency)-Reg.

Following guidelines/ recommendations have been issued by CIRA (Cyber Information Research Agency) to ensure cyber security, prevent data leakage and malware attacks:

1. Official apps should be downloaded from Google play or the App store. Third party apps should not be downloaded.

2. Opening email links should be avoided, even if the sender is familiar. Phishing is the most common delivery method for ransomware infections, delivering malware to phones and network.

3. Employees should be cautious while connected to Wi-Fi networks. Cybercriminals can access and monitor one's activity if connected to spoof networks.

4. Invest in mobile threat defense as this software will alert one to suspicious activity and fake Wi-fi networks.It also includes fully-managed restoration if data exposure were to lead to an identity theft incident.

5. Employees should be advised to avoid mixing personal with work email&/or work documents, or allowing someone they shouldn't, to use their official device or sharing official information with them through their mobile.

6. The users should exercise caution while handling and using digital assets.

7. Users should be careful while accessing internet. They should not click unwanted/unknown links.

8. The users should be careful while opening email attachment or links unless they are originated from trusted source and confirmed by the sender about the same using calling or any other kind of communication mechanism.

9. Users should not reveal personal/official information while communicating with unknown persons at social media forums.

10. Users should avoid data transmission between official and personal devices viz: USB or any other data transmitting media.

11. Users should report any suspicious cyber activity to the office as early as possible. Users should not delete or tamper any evidence in case of cyber security incident.

12. Users should follow the cyber security policies and guidelines of the organization and Government of India.

13. Users should practice data-backup with caution to have only trusted and sanitized content.

14. Use a different password for every account owned and don't save them in browser, Use a password manager to help record and manage unique passwords for every app and test password strength before using it.

15. Install antivirus software on mobile devices. As a best practice for any mobile device phones, tablets or other-consider adding antivirus software for the additional security it provides against malware or other viruses.

16. Do not "Root" the Android or "Jailbreak" the iPhone. This is a process that gives complete access of one's device, but in doing so, removes many of the safeguards that the manufacturers have put in place.

17. Always update phone's Operating System (OS) when prompted. These updates are meant to protect the device and information

18. Enable two-factor authentication (2FA) for key accounts, like mobile banking apps and peer-to-peer payment apps. This added layer of security may help prevent a thief from being able to wipe out financial accounts.

19. Revoke app permissions to use the camera, microphone, etc.

20. Be cautious to whom one is communicating in social media platforms.

The contents of the circular may be brought into the notice of all officers/officials and ensure strict adherence thereof.

(K. Haripreeti)
IDAS, DCDA

Copy to:

The officer-in-charge , IT&S Section (Local): for information & necessary action w.r.t. above as regard cyber security of the organization.

(K. Haripreeti)
IDAS, DCDA