

566
26-06-23

EDP

EDP

“ हर काम देश के नाम ”

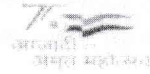
रक्षा लेखा महानियंत्रक

उलान बटार रोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt.-110010

(IT&S Wing)



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

No. Mech/ IT&S/810/Cyber Security

Circular

Date: 22/06/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)

Sub: Cyber Security Advisories.

Advisories have been circulated time to time to all the controllers regarding Cyber hygiene and to mitigate issues related to Browser attacks for NIC email accounts.

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

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

Desktop and printer security at office :

- Setup unique pass codes for shared printers.
- Always lock/log off from the desktop when not in use or before leaving the office.
- Enable desktop firewall for controlling information access.
- Ensure that the antivirus client installed on your systems is updated with the latest virus definitions, signatures and patches.
- Ensure that Operating system and BIOS firmware are updated and set BIOS password for booting.
- GPS, Bluetooth , NFC and other sensors on the desktop should only be enabled when required.
- Use of all pirated Operating systems and applications should be deleted.

Password Management :

- Use multi-factor password authentication.
- Use complex passwords and change passwords at least once in 30 days.
- Don't save passwords in the browser and don't use the same password in multiple websites/apps.

Internet Browsing Security :

- Any third party anonymization services and toolbars are prohibited in office' internet browser.
- Don't use Incognito mode while accessing govt. applications, email services or payment related services.

26/06
50 (EDP)
Pls circulate in website & whatsapp groups.
SAO (EDP)

Contd...

- c. Don't download any unauthorized or pirated content/software from internet.
- d. Don't store any username, passwords and payment related information on the internet browser.
- e. 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.

Email Security :

- a. Ensure that Kavach multi factor authentication is configured on the NIC email account.
- b. 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.
- c. Don't click any link or attachment contained in mails sent by unknown sender.

Removable Media Security :

- a. Don't plug-in the removable media on any unauthorized devices.
- b. Scan the removable media with Antivirus software before accessing it and perform a secure wipe to delete the contents of the removable media.

Security Advisory and Incident Reporting :

- a. Adhere to Security advisories published by NIC-CERT (<https://niccert.nic.in>) and CERT-In(<https://cert-in.org.in>)
- b. 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.

D. Browser in browser Phishing Attacks for Nic email accounts :

- a. Emphasis on checking the URL of the site and that the site's URL shows 'https' with accompanying padlock indicating that the site is secured.
- b. It is requested to avoid clicking on any suspicious links in emails.

E. Cyber Security Best practices : Social Media advisories :

- a. Privacy settings are to be carefully set and reviewed regularly.

- b. Once information is posted on social media, it is difficult to delete/remove, hence be very cautious while posting photos, comments.
- c. In case of any suspicion regarding the sites you have visited or person with whom have shared information, intimate your seniors and take remedial actions.
- d. Social media is not to be used for exchange of service related information including leave, temporary duty, move etc. Always be cautious and consider that you are being monitored by advisories.
- e. Please be aware of various provisions of Information Technology Act 2000/2008 and Official Secrets Act 1923 while giving information and expressing views on social media.
- f. Don't respond to unsolicited emails and junk email(spam). Don't unsubscribe from their emailing list that just let the spammer know that they have found the valid email address. The safest path is to ignore and delete it.

F. Cyber Security Measures- Smart TVs and Smart Boards :

- a. Ports of smart TV should be connected to the intended source only, under no circumstances, a smart TV is to be used for displaying data from two different sources.
- b. Disable Bluetooth and Wi-Fi connections unless deemed necessary. Download only trusted applications. No sensitive information/service related content to be stored in smart TV/board.

G. Attempts by Pakistani Intelligence Operatives :

- a. Pakistan Intelligence Operatives to particularly target officials posted in sensitive organizations by honey trapping them over social media.
- b. PIOs are using fake identities, including posing as defence correspondents of Ministries and are using spoofed numbers to gain the trust of unsuspecting individuals to ferret out sensitive information. It is requested to sensitize all personnel in organizations under your control to remain vigilant.

H. Cyber Security Alert-Phishing Mail :

- a. Any email with the suspicious phishing link should not be clicked , the particular link may be compromised . It is requested to sensitize all officials not to click on any such link and also to report to incident@nic.cert.nic.in .

I. Phishing Domains used by Chinese threat Actors:

- a. It is requested to-avoid communication with the following mentioned list of domains and email ids:

Domains :

- drive-nic.online
- files-nic.link
- files-nic.space
- mydrive-nic.com

- mydrive-nic.space
- secure-nic.online
- attachment-nic.online
- see-nic.online
- cloud-nic.online
- mydrive-nic.online
- files-nic.online
- myfiles-nic.space
- nic-files.download

Email ID's :

- jack16666@yahoo.com
- elein16666@hotmail.com
- frankli1995@yahoo.com
- jameschen1997@yahoo.com

J. Usage of m KAVACH 2.0 Application on Personal android mobile phones :

- a. It is advised to download m Kavach 2.0 application on personal android mobile phones. Its security features are threat analyzer, detection of hidden and banned applications, security advisor , app statistics etc.

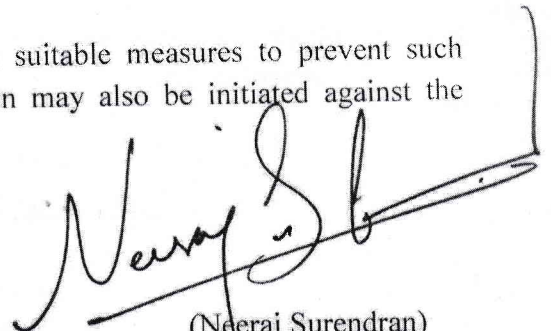
K. Mobile based malware methods and countermeasures :

- a. Users should always keep updated OS and all the updated apps in the mobile.
- b. Users should use strong login passwords and biometric authentication.
- c. Disable third party app stores or any other unknown standalone source as they can be vectors for spreading malware.
- d. Pay attention to the permission asked by the apps while installing and review them periodically.
- e. Disable radio services like Bluetooth, Wi-Fi , GPS and NFC when not required. Also, avoid connecting to public Wi-Fi which is often not secured and is a very common attack vector.
- f. Security Software protects against malware infection and should be installed from verified vendors/sources.
- g. It is advised to use the genuine charger and connect cables only for a trusted PC/laptop for charging or data transfer. Avoid charging your mobile phones at public charging stations.
- h. Be careful about hyperlinks and ads. Inspect links thoroughly before clicking.
- i. Avoid jailbreaking or rooting your phone to gain access to some access to some applications or services.
- j. It is advised to delete all the data from the mobile device before discarding the device so as to ensure data is not misused.
- k. Users who suspect their smartphones to be infected are advised to visit the "Cyber Swachhta Kendra" website <https://www.csk.gov.in/security->

[tools.html/](#) and download free bot removal tools. Users can scan and remove bots from their devices using these tools.

- l. It is advised to disable the ad identifier "IDFA(identifier for Advertisers)" on ios or "AAID(Android Advertising ID)" on android. It will make it substantially harder for advertisers and data brokers to track profile of the user and it will limit the amount of personal information that reaches the advertisers.
 - m. Install security software from verified vendors/sources. Additionally it is advised to install mKavach 2.0 application in personal mobile phone.
3. It is also requested to follow the guidelines mentioned in the even numbered circular dated 24/08/2022 and 16/03/2023 mentioning issues related to whatsapp squatting and ransomware attacks.
4. Further, it is also directed that apart from taking suitable measures to prevent such incident in future, administrative/disciplinary action may also be initiated against the individual prima facie responsible.

Jt. CGDA (IT&S) has seen.



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