

CGDA Query/08
26/02/2021

AOI EDP Q1
01/03

**CONTROLLER GENERAL OF DEFENCE ACCOUNTS – IT&S
ULAN BATAR ROAD, PALAM, DELHI CANTT – 110010**

Phone : 011-25665761-63 Fax : 011-25675030

Website : <http://cgda.nic.in>

Email : cgdanewdelhi@nic.in

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

Dated: 18/02/2021

To

All PCsDA/CsDA/PrIFAs/IFAs/PCA(Fys)

Subject : Cyber Security Advisory- : Fake Messaging App "WHSAPP.APK".

It has been noticed that a Netherlands and Bulgaria based file named Whsapp.apk embedded with malicious content is being circulated on Whatsapp Groups amongst defence personnel which is asking the following permission of android devices :

- (a) Access the Internet
- (b) Access Network State
- (c) Access/Change wifi state
- (d) Modify fine loc
- (e) Record Audio
- (f) Read call log
- (g) Read Contact
- (h) Write/Reader to external storage
- (j) Write/Read SMS.

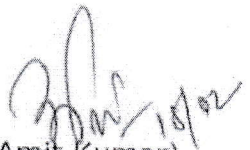
Go (IT)
for circulation
L
compliance
by
26/2

In view of the above, following action points are recommended

- (i) Not to access/install any app on android devices received from unauthorized sources.

To (IT)
for n/w
2/2

- (ii) Not to download attachment or click on any hyperlink received from suspicious email. The said email required to be forwarded to CIRA for analysis at advcyber.tech@gov.in.
- (iii) IP Address 178.132.3.230 and 89.45.67.50 should be blocked at all computer / internet firewall to prevent any communication.
- (iv) Change login credentials immediately if suspicious attachment downloaded / clicked on hyperlink.
- (v) Always verify sender's credentials / details.
- (vi) Change user credentials for bank acct, email and other online services regularly.
- (vii) System should be updated with latest security patches and AV updates.


(Amit Kumar)

Sr.ACGDA(IT&S)