F. No. 1-5/2003/24(NTISB-II)   Islamabad, the 1st April, 2024

22 APR 2024

Subject: - **Cyber Security Advisory – Hostile APTs Targeting Pakistani Officials with Android Apps for Data Exfiltration Via Google Play Store (Advisory No. 06)**

Context. Reportedly, a number of suspicious android applications on Google Play store have been identified. These applications (**Annex-A**) are designated to extract personal/financial data including media, contact list, calendar, call/message logs etc. from the victim's mobile phones upon downloading (without user consent). Moreover, some of the apps also offer to provide Personal Identifiable Information (PII) of Pakistani citizens on demand in lieu of monetary exchange. Therefore, a cautious approach is essential in usage of such apps.

2. **Preventive Measures**

a. No applications from unknown source/3rd party hosting (except from Google Play Store) be installed on Android phones.

b. While downloading and installing new applications, user must check reviews privacy policy and avoid providing phone number/email addresses.

c. Keep thorough check on permissions granted to all the installed applications including system applications and change the phone, if any suspicion arises.

d. Before installation of any applications, users must read its privacy policy; what data is collected from users and with whom it is being shared.

e. Google play protect (Android built-in Antimalware) must not be switched off in any case.

f. Do not open emails and attachments from unknown or suspicious sources.

g. Update mobile operating system whenever updates are available.

h. Do not keep official data in smartphone in any case.

M (IR-Ops)	
M (IR-P)	
M (Cus-Ops)	
M (Cus-P)	
M (Admn/HR)	✓
M (IT)	✓
M (FATE)	
M (Legal)	
M (Reforms)	
M (Legal & Acc. Cus)	
M (Acc & Audit)	
Addl. Secy (Rev.Div.)	✓
SA / SPS	

i. Keep smartphone's location turned off all the time and do not carry smartphone to any sensitive location/setup.

j. Ensure strong passwords on general security policies.

k. Install good antivirus and anti-malware software and update signature definitions in timely manner.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.