Subject: **Advisory – Prevention against SMS Scam Apps (Advisory No. 70)**

1. Subject advisory is attached at **Annexure-A**.

   a. **C&IT Coord** Contents may be shared with following addresses: -

      (1) Inspector Gen, C&IT Branch GHQ

      (2) Dir CSO, C4I Dte C&IT Branch GHQ

   b. **MI Coord** Contents may be shared with following addresses: -

      (1) DMI Tech, MI Dte

      (2) CO Unit-22, MI Dte (MI-22)

   c. **MO Coord** Content may be shared DMO (Ops), MO Dte.

   d. **Naval Headquarters** Contents may be share with following addresses: -

      (1) DG NI Naval Headquarters

      (2) DG C4I Naval Headquarters

      (3) Director Cyber Security Naval Headquarters

   Air Headquarters Contents may be shared with following addresses: -

      (1) DG AI, Air Headquarters

      (2) DG C4I, Air Headquarters

      (3) ACAS (NCW) Secretariat

   f. **SPD** Content may be shared HQ CSD / HID, SPD

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

Annexure-A

1. Recently, a fraud campaign is spreading globally through **social engineering tactics; 151x malicious Android applications (10.5 million downloads)** have been observed enticing users for premium subscription services. The **Identified applications (examples at Appendix-I)** are dubbed as **UltimaSMS Apps** which cover wide range of categories such as **keyboards, QR code scanners, video** and **photo editors**. These applications target users through SMS and ask them to enter their phone numbers and email address to gain access to the advertised features. Therefore, recommendations mentioned below must be followed to avoid becoming victim of such applications.

2. **Recommendations**

   a. **No applications from unknown source** (except from **Google Play Store**) be installed on Android phones.

HR eDOX Dy.No. 186034/21
ceived in Chairman's Sectt
08 NOV 2021

11/11/21

12-11-21

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

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

d. Disable premium **SMS** option with the carriers to prevent subscription abuse

e. **Google Play protect** (android built in Antimalware) **must not be switched off in any case**.

f. Update mobile operating system whenever updates are available.

g. Use antivirus to prevent personal data loss / infection.

Appendix-I

EXAMPLE MALICIOUS ANDRIOD APPLICATIONS

Serial	Application
1.	Ultimate Keyboard 3D Pro
2.	Video Mixer Editor Pro
3.	FX Animate Editor Pro
4.	Battery Animation Charger
5.	Dynamic HD & 4k Wallpapers

3. **Reporting of Suspicious Files / Emails** Any malicious activity may be reported on following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

4. Forwarded for information / dissemination to concerned, please.

Subject: **Advisory – Prevention against SMS Scam Apps (Advisory No. 70)**

1. Subject advisory is attached at **Annexure-A**.

a. **C&IT Coord** Contents may be shared with following addresses: -

(1) Inspector Gen, C&IT Branch GHQ

(2) Dir CSO, C4I Dte C&IT Branch GHQ

b. **MI Coord** Contents may be shared with following addresses: -

(1) DMI Tech, MI Dte

(2) CO Unit-22, MI Dte (MI-22)

c. **MO Coord** Content may be shared DMO (Ops), MO Dte.

M (IR-Ops)	d
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.)	✓
SO / SPS	

Naval Headquarters Contents may be share with following addresses: -

(1) DG NI Naval Headquarters

(2) DG C4I Naval Headquarters

(3) Director Cyber Security Naval Headquarters

Air Headquarters Contents may be shared with following addresses: -

(1) DG AI, Air Headquarters

(2) DG C4I, Air Headquarters

(3) ACAS (NCW) Secretariat

f. **SPD** Content may be shared HQ CSD / HID, SPD

Annexure-A

1. Recently, a fraud campaign is spreading globally through **social engineering tactics; 151x malicious Android applications (10.5 million downloads)** have been observed enticing users for premium subscription services. The **Identified applications (examples at Appendix-I)** are dubbed as **UltimaSMS Apps** which cover wide range of categories such as **keyboards, QR code scanners, video** and **photo editors**. These applications target users through SMS and ask them to enter their phone numbers and email address to gain access to the advertised features. Therefore, recommendations mentioned below must be followed to avoid becoming victim of such applications.

2. **Recommendations**

a. **No applications from unknown source** (except from **Google Play Store**) be installed on Android phones.

9/11 DS(IT) 9/11/21