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

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.

   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