Subject: **Prevention Against Android Bankosy Malware - (Advisory No. 06 Feb 2016)**

1. **Introduction.** A new android malware has been reportedly detected and found effective. The malware is known as Android. Bankosy and is designed to mislead voice call-based two-factor authorization (2FA) systems and is targeting Android devices.

2. **Method of Infection**. Android. Bankosy malware can infect the device in various' methods. Some of them are given below:-

a. Phishing emails / sites.

b. Fake SMS.

c. Mobile applications downloaded from free websites.

3. **Method of Operation**. Following method enables the respective malware to infect the system:-

a. Once the malware is installed on a compromised device, the malware collects a list of system-specific information, and sends it to the attacker's server to register the device.

b. The attacker's server then sends a unique identifier to the compromised device in order to further hack the devices.

4. **Capability**. Android Bankosy has following abilities:-

a. Intercepts incoming SMS.

b. Deletes SMS messages.

c. Wipes data.

d. Deceives voice call based 2FA systems.

e. Enables call forwarding on the infected device.

f. Provides support to enable and disable silent mode and to lock the device.

5. **Recommendations.** To protect against Android Bankosy on mobile devices, following measures should be taken:-

a. Update android operating system and applications.

b. Refrain from downloading apps from unfamiliar sites.

c. Only install apps from trusted sources (Google play store).

d. Install a suitable mobile security app, in order to protect the device and data.

e. Make frequent backups of important data.