Subject: **Cyber Security Advisory - Prevention against Indian Oriented Social Media Mobile Application- Crazy Talk (Advisory No.03)**

1. **Introduction.** Recently, it has been observed that an **Indian origin 3rd party Social Media Android application "Crazy Talk"** is being used by users for sharing messages, images and voice / video calls. This application is not available on Google Play store and may be downloaded from 3rd party servers.

2. **Feature - Crazy Talk Application.** The application seamlessly uploads sensitive information of the users like contacts, call logs, SMS, WhatsApp / signal data, medial files and documents to its own server.

3. **Best Practices / Recommendations for Mobile Application Usage.**

a. **Block installation of all applications from unknown sources,** these options are disabled in Android by default and it should stay that way.

b. Only install application from official App Stores / Google **Play Store.**

c. **Google Play protect** (Android built in Anti Malware) **must not be switched off** in any case. It detects suspicuous looking apps in mobile device based on their behavior and generates alerts for user.

d. **Do not click on links that promise unusual features or functionalities** such as **"whatsApp offers of free Airline Tickets"** are usually just an attempt to steal your personal data. The same applies to phishing including texts form frineds containing suspicious URLs.

e. Before installing any application,**user must read its privacy policy explaining what data it collects form users and with whom it is sharing that data.**

f. It is strongly recommended to all users to ensure keeping their **communication app up to date form their respective App Stores. Do not ignore updates from apps installed on your device.**

g. **Regularly Update Mobile Operating System** whenever updates are available.

h. **Install Antivirus** on mobile device to prevent any danger that may affect your personal data.

i. **Carefully consider what information you want to store on the device** as an attacker can obtain your stored information through cleverness.

j. **Be careful when using social networking apps;** these apps may reveal personal information to unintended parties. Be especially careful when using services that track your location.

4. **Reporting of Cyber Security Issues / Queries**. For reporting malware or any other query or issues regarding Cyber Security, details may please be forwarded to the following email address.

asntisb2@cabinet.gov.pk

5. Disseminate the same to attach / affiliated, departments and branches, forwarded for necessary action, please.