Subject: - **Cyber Security Advisory - New Malware/ Suspicious Appl "Nebula Shopping" (Advisory No. 24)**

Introduction. A **3rd party** application **Nebula Shopping** is targeting applicants/ users to acquire their personal and financial details such as **mobile phone number, bank account** and **email ID;** thereby making users vulnerable to **identity theft** and **fraud.** Such applications with other names can also be found on the web. Cyber probe and technical analysis against Nebula Application revealed that Nebula Shopping is allegedly a fraud application for earning money online and aims to provide easy loan through online order submission.

2. **Recommendations**

a. **Don't Reveal Personal** or **Financial Information on 3rd Party apps.** Do **not respond** to **Application solicitation** for this information.

b. **Check security permissions of such apps** before providing any sensitive information online.

c. In case, a user is not sure whether the app is legitimate, **try to verify by contacting the company directly**.

d. **Block installation of apps from unknown sources**, only install apps form official app stores, such as **Google Play Store/ App Store**.

e. **Google Play project** (android built in Anti Malware) **must not be switched off** in any case as it detects suspicious apps in your mobile device based on their behavior and generates alerts.

f. Before installing any app, **users must read its privacy policy explaining what data it is collecting form users and with whom it is sharing that data.**

g. It is recommended that users should keep their **communication app up-to-date from their respective App Stores. Do not ignore updates from apps installed on your device.**

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

i. **Use Antivirus** in order to prevent any danger that may compromise personal data stored on the device.

j. **Carefully consider what information you want to store on the device,** remember that with enough time, sophistication and access to the device, any attacker can obtain the stored information.