Cyber Security & IT Examination Cell
साइबर सुरक्षा एवं सूचना प्रौद्योगिकी परीक्षा कक्ष

Confidential

Alert No: 1/2019 **Dated: February 14, 2019**

New Modus Operandi to commit Fraud in Digital Payment Ecosystem

Fraudulent transactions using the UPI platform are increasing. We have issued advisory no.1 dated January 10, 2019 in this regard.

Recently, a new modus operandi has been brought to our notice through which fraudster can easily take remote access of a victim's mobile device and carry out transactions. Stepwise details are as under:

- Fraudster would lure the victim on some pretext to download an app called 'AnyDesk' from Playstore or Appstore. It may be noted that, there are more apps similar to 'AnyDesk' that help provide remote access of device to other users.
- The app code (9 digit number) would be generated on victim's device which the fraudster would ask the victim to share.
- Once fraudster inserts this app code (9 digit number) on his device, he would ask the victim to grant certain permissions which are similar to what are required while using other apps.
- Post this, fraudster will gain access to victim's device.
- Further the mobile app credential is vished from the customer and the fraudster then can carry out transactions through the mobile app already installed on the customer's device.

Above modus operandi can be used to carry out transactions through any Mobile Banking and Payment related Apps (including UPI, wallets etc.)

In this connection, banks are advised to take necessary measures to create customer awareness so as to minimize/eliminate above frauds.

----------x----------