Digital Payments Safety Initiative by NPCI

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 Banking transactions.

Stepwise details are as under:

- Fraudster 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 (By Calling) 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.)

Customers need to stay alert and do not use 'AnyDesk' (or any other similar) app to minimize/eliminate above frauds. And, follow below listed instructions:

- Always install applications downloaded from reputed application market only, like Google Play Store, Apple app store.
- Never install applications through link sent by unknown person on Whatsapp, Facebook, SMS, etc.
- Never respond to message / people posing as Bank official through SMS (Short Message Service), text message, telephone call, fax, voicemail etc.
- Do not store Bank account number/Customer ID or MPIN / PIN / Card Details in the mobile phone.
- Do not share Bank account number/Customer ID or MPIN / PIN / Card Details with anyone.