Karnataka Bank Ltd.

Your Family Bank, Across India

New techniques used by fraudsters in Digital Ecosystem

Recently, a new method of carrying out fraudulent transactions has been observed in mobile banking and payment related applications like UPI etc . In this technique, a 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 Google Playstore or Apple Appstore. It may be noted that, there are more apps similar to "AnyDesk" that help to 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 the 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 carry out transactions through the mobile app already installed on the customer's device.

It is also being observed that a number ***"06206419089"*** is being updated as customer care number of multiple Banks', Google Pay and IRCTC on Internet Search Engines, kindly beware of such fraudulent customer care number do rely on Bank's corporate website for customer care contact details.

In view of the above, we request you to please exercise utmost caution to thwart any attempts from unscrupulous elements resulting in financial losses.

SEC_RITY IS NOT COMPLETE WITHOUT U.

BEWARE OF WHAT YOU SHARE.