यूनियन बैंक ऑफ इंडिया Union Bank of India

Security Alert – Frauds committed via Mobile Application

Fraudulent transactions in digital payment ecosystem have been on the rise. A new modus operandi has been reported 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.)

Precautions:

- Do not download any unknown/suspicious application without verifying its genuineness.
- Do not grant unwanted permissions which grant remote access.
- Do not share any confidential bank details like debit card number, card expiry date, CVV, OTP, Password, ATM PIN etc. with anyone over call, SMS or email.
- Do not click on suspicious links in SMS or MMS sent to your mobile phone.
- Always keep device OS and antivirus up to date.
- Always keep strong and unique password for mobile as well as for payment related applications.
- Avoid using unknown/unsecured Wi-fi hotspots and keep your Wi-fi turned off when not in use.
- Turn off “Allow installation of Apps from sources other than the Play store” option under Settings -> Security.