बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

Dear Valued Customer, 04.05.2020

Thank you for banking with Bank of Maharashtra.

Security of your account is of utmost importance to us. In our endeavour to continue educating our customers on security, we are hereby publishing the Customer Awareness - 15. Hope you will find it useful and informative.

Quick Support -Team Viewer App – Cyber Fraud

Fraudulent transactions using the UPI platform/Mobile Banking are reported to be increasing. The apps such as Quick Support–TeamViewer, AnyDesk, etc. are being misused for taking remote control of the device to carry out fraudulent transactions. We are giving below modus operandi in this regard for your information and awareness and making you alert about the same.

Modus Operandi

A SMS is received on customer’s mobile stating that his PayTM transactions are suspended/blocked as his KYC verification is pending. A contact number is also provided, thereby inviting the customer to contact the fraudster.

- The fraudster poses himself as the customer care executive and insists the customer to complete the KYC verification on his own by installing Quick Support -Team Viewer or Anydesk App on his mobile. The customer gets convinced as he does not have to reveal any confidential information.
- The app code would be generated on victim's device which the fraudster would ask the victim to share.
- Once fraudster inserts this app code on his device, he would ask the victim to grant certain permissions which are similar to that are required while using other apps. Post this, fraudster will gain access to victim's device.
- Further the mobile app credentials would be collected 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.) already installed on Mobile.

To avoid falling prey to this scam, following measures shall be followed:

- Avoid downloading Quick Support -Team Viewer ‘AnyDesk’ or similar app from Playstore or Appstore on suggestion over phone.
- Do not grant unwanted permissions for remote access.
- Do not share the credentials (OTP,PIN, Card number, CVV number, card expiry date, etc.) with anybody over any mode.
- Keep strong and unique passwords for mobile and each payment related apps.
- Keep Operating System of Mobile device and antivirus up-to-date.

-By Chief Information Security Officer, Bank of Maharashtra