New Modus Operandi to Commit Fraud in Digital Payment Ecosystem - Through 'AnyDesk' Mobile App

A new modus operandi has been observed through which fraudsters can easily take remote access of mobile device and carry out fraudulent transactions. The modus operandi is explained below (along with preventive actions):

Sl No	Modus Operandi	Preventive Action
1.	Fraudster would lure the victim to download an app called 'AnyDesk' from Playstore or Appstore. There are more apps similar to 'AnyDesk' that help provide remote access of device to other users.	Don't download 'AnyDesk' or similar app from Playstore or Appstore. This may lead to fraudulent transaction in your account.
2.	The app code (9 digit number) would be generated on victim's device which the fraudster would ask the victim to share.	Don't respond to fraudster's call (through Mobile, SMS, or Email) and don't share any details with them through any mean.
3.	Once fraudster inserts this app code (9 digit number) on his device, he would ask the victim to grant certain permissions.	Don't respond to fraudster's call to grant any permission on mobile.
4.	Fraudster will gain access to victim's device.	As above.
5.	The mobile app credential is vished from the customer and fraudster then carry out transactions through the mobile app already installed on customer's device.	Never share your Mobile Banking and UPI login credentials over Call, SMS or Email.

Note: Sarva Haryana Gramin Bank will never send you e-mails, SMS, or call you asking for confidential details of your account/ PIN/ Password/ OTP or personal details such as date of birth, mother's maiden name etc. Beware of anyone asking you for such information on behalf of the Bank through e-mails, phone calls, or SMS.