BEWARE OF COVID THEMED CYBER-ATTACKS.

Some fraudsters are more virulent than Corona.

We are in uncharted territory due to COVID-19. It is noticed that some fraudsters are trying to cash in on your fear of COVID. Your banking safety is in your hands. Please take the following precautions.

- Never open attachments of a mail especially Coronavirus themed phishing mails claiming to be from World Health Organization (WHO) or other Government and such related authorities, where the sender is unrecognized /unknown/doubtful.
- Always secure digital transactions using "e-lock" feature in the bank's Mobile App "SIB Mirror+". e-lock is enhanced to set a limit for digital channel transactions.
- Customers are advised not to open attachments in unsolicited emails/SMS, even if the email/SMS seems to be from your contacts. Never click on the URLs in those emails/SMS and be vigilant of suspicious attachments.
- Make sure you know which site a link is taking you to before you click on it. Hover the cursor over the link for a few seconds until the link's URL pops up and confirm that the link leads to a site that you recognize. It is strongly recommended to avoid clicking on any links embedded in emails.
- Customers are advised to use their UPI PIN only to send money/make UPI payments for some services. Never enter the UPI pin to receive money from any sources. Also, customers need to scan the QR Code only to make payments and do not scan any QR code from any source to receive money.
- Customers are advised to always use strong passwords and regularly change the passwords of your devices/online accounts. The same password should never be used at multiple sites. Please do not store the password in mobile phones, diary etc.
- It is strongly recommended to enable multifactor authentication wherever possible in online accounts.