इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

Financial Scams - COVID 19 Pandemic

Dear Customer,

The cyber-attacks have been rapidly increasing during worldwide pandemic COVID 19 and targeting continuously you. The Steps to avoid Financial scams-

- Don't respond to **phishing** e-mail/ SMS: Do not click the URL which you receive from unknown sources or open suspicious attachments. Don't disclose personal information or online banking credentials via e-mail or text message as these might be used for identity theft.
- **Vishing** or beware of verification calls**:** The fraudster usually pretends to be our bank official/ IT personal. After giving a false sense of security, the fraudster then tricks you into giving away your personal and confidential data. When in doubt, always call or email your nearest branch official and ask them about the call.
- **UPI fraud,** fraudsters could ask you to click on links, accept 'collect request' received over text messages and enter UPI MPIN (mobile banking personal identification number). Fraudsters could also ask to share debit card details, text messages, UPI registration OTP, passcode, and password and use this data to create a new virtual payment address (VPA) ID and set MPIN. Beware and don't disclose your UPI MPIN.
- *Do not share **your OTP to avail EMI moratorium**: Our bank will never call you or send you an email for your OTP or password details to postpone your EMI. Never share your personal information like debit/credit card numbers, CVV numbers, internet banking/mobile* banking password, PIN, One Time Password (OTP), UPI PINs etc. with anyone asking for verification over phone, email or bank employees at branches.
- **Disable the 'Auto Save' or 'Auto Complete'** features on your internet banking site/ mobile banking app: Do not enable auto-fill or save user IDs or passwords for internet banking or mobile banking transactions. Though it's convenient to use but it can be risky.
- **Skimming:** The fraudsters skim information from cards, using devices stealthily installed in ATMs or at physical stores. Fraudulent online transactions can be done using skimmed data and confidential information.
- Conduct **account check-ups** through mPassbook/ Nanban/ Internet banking/ Mobile banking App: It is equally important to be aware about your financial health. Regularly check your bank accounts to keep a track of your money. Each time you make a transaction, go back and check the balance to ensure that right amount has been paid or received. If unreachable over all means, then contact over phone to nearest branch.

The fraudsters keep coming up with new techniques to defraud. So, it is important to be informed, and safe and secure in our financial transactions.

Branch Manager