DCB BANK

Annexure 7: Consumer Awareness - Cyber Threats and Frauds

It has been observed that unscrupulous elements are defrauding and misleading the public by using innovative modus operandi including social media techniques, mobile phone calls, etc. In view of this, DCB Bank cautions the public to be aware of fraudulent messages, spurious calls, unknown links, false notifications, unauthorised QR codes, etc., promising help in securing concessions/ expediting response from banks and financial service providers in any manner.

Fraudsters attempt to get confidential details such as user id, login and or transaction password, One Time Password (OTP), debit and credit card details such as PIN, CVV, expiry date and other personal information. Typical modus operandi being used by fraudsters are:

- Vishing - phone calls pretending to be from bank, non-bank e-wallet providers, telecom service providers to lure customers into sharing confidential details under the pretext of KYC-updating, unblocking of account, SIM card, crediting debited amount, etc.
- Phishing - spoofed emails and or SMS designed to dupe customers into thinking that the communication has originated from their bank or e-wallet provider and contain links to extract confidential details.
- Remote Access - by luring customers to download an application on their mobile phone and, or computer which can access data in the customer's device.
- Misuse the 'collect request' feature of UPI by sending fake payment requests with messages such as, 'Enter your UPI PIN' to receive money.
- Fake contact numbers of banks and e-wallet providers on webpages and social media and displayed by search engines, etc.
- Investment frauds: Trick customers into making financial investments under false pretenses, such as promises of high returns with low risk, often leading to loss of funds.
- Mule accounts: Using bank accounts of customers often without their knowledge to launder or transfer illicit funds.

DCB Bank urges the public to practice safe digital banking by taking all due precautions, while conducting any digital (online, mobile) banking and payment transactions. These will help in preventing financial and other loss.

SAFE DIGITAL BANKING PRACTICES

- Never share your account details such as, account number, login ID, password, PIN, UPI-PIN, OTP, ATM, Debit Card, Credit Card details with anyone, not even with bank officials, however genuine they might sound.
- Any phone call or email threatening the blocking of your account on the pretext of non-updation of KYC and suggestion to click link for updating the same is a common modus operandi of fraudsters. Do not respond to offers for getting KYC updated or expedited. Always access the official website of your bank, or contact the branch.
- Do not download any unknown app on your phone or device. The app may access your confidential data secretly.
- Transactions involving receipt of money do not require scanning barcodes or QR codes or entering MPIN. Thus, exercise caution if asked to do so.
- Always access the official website of the bank, for contact details. Contact numbers on internet search engines may be fraudulent.

- Check URLs and domain names received in emails and SMS for spelling errors. Use only verified, secured, and trusted websites and apps for online banking, that is, websites starting with ‘’https’’. A suspicious URL or website should be notified to local police/ cybercrime branch immediately.
- If you receive an OTP to debit your account for a transaction not initiated by you, inform your bank or e-wallet provider immediately. If you receive a debit SMS for a transaction not done, inform your bank/ e-wallet provider immediately and block all modes of debit, including UPI. If you suspect any fraudulent activity in your account, check for addition to the beneficiary list enabled for internet and mobile banking.
- Do not share the password of your email linked to your bank or e-wallet account. Do not have common passwords for e-commerce and social media sites and your bank account and email linked to your bank account. Avoid banking through public, open or free Wi-Fi or internet networks.
- The password used for accessing your email, especially if linked with your bank account, should be unique and used only for email access and not for accessing any other website or application.
- Do not be misled by advice intimating deposit of money on your behalf with RBI for foreign remittances, receipt of commission, or wins of lottery, misleading advertisements (including ads for offers / discounts).
- Regularly check your email and phone messages for alerts from your financial service provider. Report any un-authorized transaction in your account to your bank, NBFC or service provider immediately for blocking the card, account, wallet, to prevent further loss.
- Secure your ATM, Debit and Credit Cards and set daily limit for transactions. You may also set limits and activate or deactivate for domestic or international use. This can limit loss due to fraud.

*****