NAV JEEVAN CO-OP. BANK LTD.

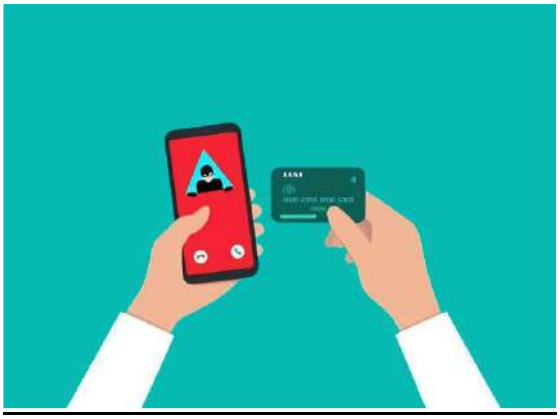
BHAWANI SAW MILLS COMPOUND, FURNITURE BAZAR, ULHASNAGAR – 421003

CYBER SECURITY – FRAUDS - DO's and DON'T'S

Phishing Links / Emails / SMS:

- DO NOT click unknown links and delete the SMS / email immediately to avoid accessing them in future. Verify the website details especially where it requires entering financial credentials.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform.
- Beware of any SMS/Call/Social Media Message promising high returns on Investment and legal action/fine from CBI, Income Tax etc. In case of such incident, report immediately to 1930 or cybercrime.gov.in

Vishing calls:



- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.

Online Sale Fraud:

- Be careful while making financial transactions for online products.
- Always remember, to receive money there is no need to enter your PIN / password anywhere.
- If UPI or any other app asks you to enter your PIN to complete transaction, it means you will end up sending money instead of receiving it.

Frauds due to the use of unknown / unverified mobile apps:

- Never download an application from unverified / unknown sources.
- Before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions, which are absolutely required to use the desired application.

ATM card skimming:

- Verify to ensure that there is no extra device attached near card insertion slot or keypad of ATM machine while making transaction.
- Cover the keypad with your hand while entering your PIN.
- Do NOT enter the PIN in the presence of any other person standing close to you or share the card with anyone.
- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.

- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.

Frauds using screen sharing app / Remote access:

- In case you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen-sharing app is removed from your device.
- Do not download or activate share screen share feature with unknown people.
- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.

SIM swap / SIM cloning:

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number

Frauds by compromising credentials on results through search engines:

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as fraudsters often camouflage these.
- Please also note that customer care numbers are never in the form of mobile numbers

Scam through QR code scan:

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.

Impersonation on social media:

- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.

Juice jacking:

- Avoid using public / unknown charging ports / cables.

Online Job Fraud:

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.

Online Lottery Frauds:

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.

Money Mules:

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorized money and to transfer them to others or withdraw cash and give it out for a handsome fee.

- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.