SECURE BANKING

Bharat Bank's online services (Netbanking & Mobile Banking) are safe and secure. Bank has ensured safety measures to protect your personal information with the Bank.

In addition to this customer has to be vigilant about frauds and scams to ensure complete safety. Please note the following safety measures to ensure safety of your account & online transactions.

- Do not click on links in the SMSes informing you that your account will be blocked if you do not update KYC/PAN/Aadhaar details.
- Scamsters may advise you to download apps to help resolve your complaints. By downloading and installing such apps, they may get access to your mobile screen and other mobile data.
- Scamsters update fake helpline numbers on forums, fake websites, google maps etc. Do not call such numbers. Refer only to Bharat Bank's official website https://www.bharatbank.com for official helpline numbers of the Bank.
- Do not share your Customer ID and login password, OTP, ATM PIN, card number, CVV, expiry date, UPI VPA/MPIN with anyone over message, call, email, etc.
- Do not click, open, or respond to emails, messages, links, etc., with lucrative offers, cashback, discounts, rewards points, loans with low-interest rates, etc.
- Ensure that the URL of the Bank's Website is https://www.bharatbank.com/
- SMSes from Bharat Bank will always include a header like XX-BCBANK, where XX is a variable.
- You need not enter UPI PIN or scan QR code to receive payments through UPI.

MOBILE SECURITY:

DO's

- Password protect your mobile phone.
- Choose a strong password to keep your account and data safe
- Review your account statements frequently to check for any unauthorised transactions
- Change your IPIN regularly
- Report a lost or stolen phone immediately to your service provider and law enforcement authorities

DONT's

- Never give your PIN or confidential information over the phone or internet. Never share these details with anyone
- Don't click on links embedded in emails/social networking sites claiming to be from the bank or representing the bank
- Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed
- Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone
- Don't forget to inform the bank of changes in your mobile number to ensure that SMS notifications are not sent to someone else
- Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password

- Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources
- Be cautious while using Bluetooth in public places, as someone may access your confidential data/information
- Be careful about the websites you are browsing. If it does not look authentic, do not download anything from it.

FRAUDS:

Identity Theft

- Destroy any piece of paper that contains your login and password.
- Never share your personal information with a stranger or any third party.
- Update your bank records whenever you change your contact numbers, address or email ID.

Vishing

- Fraudsters call you, posing as government or bank employees.
- Never share any personal or sensitive information over a call.
- If in doubt, call the bank's PhoneBanking number.

Smishing

- Never share your personal or financial information via SMS.
- Do not follow instructions that you receive in an SMS from an untrusted source.
- If you receive any urgent communication asking for personal information, call and confirm with PhoneBanking.

SECURITY TIPS:

ATM BANKING:

- Memorise your PIN. Do not write it down.
- Do not share your PIN with anyone.
- Do not take help from strangers for using the ATM card or handling your cash.

SECURE COMPUTER:

- Use licensed software.
- Use anti-virus, anti-spyware and personal firewalls.
- Protect your computer accounts with strong passwords.

SECURE NETBANKING:

- Do not disclose your customer ID and IPIN to anyone
- Change your IPIN as soon as you receive it the first time
- Avoid accessing NetBanking over shared networks at cyber cafes, airports etc.
- SECURE INTERNET BROWSING
- Don't download software or content from untrustworthy sites
- Don't click on links that you do not trust

- Read the privacy policy of a website before providing personal information

MOBILE SECURITY

- Protect your phone with a strong screen password
- Report lost or stolen phone immediately
- Change your IPIN regularly

ONLINE SHOPPING

- Always shop or make payments through trusted/reputed websites
- Sign up for Verify by Visa and Master Card secure code program
- Before entering your private details, always check the URL of the site you are on!

PASSWORD SECURITY

- Don't use predictable password such as DOB or family member's name
- Use a mix of alphabets, numbers, uppercase, lowercase and special characters
- Memorise your password. Don't write it down.

SECURE PHONE BANKING:

- Never reveal any password or code to a phone banking officer
- Avoid giving verification details to the officer while in public
- Do not transfer the line or hand over the phone to any other person after you complete self-authentication

FRAUDS / CYBERCRIMES THROUGH INVESTMENT / PART TIME JOB / PONZI SCHEME SCAMS

Based on reports of various frauds / cybercrimes, Regulatory authorities have identified modus-operandi adopted by fraudsters and criminals through investment / part time job / Ponzi schemes to defraud/cheat the public as under:-

a) Victims are lured through part-time job offers and other advertisements on internet and/or messaging platforms etc. and are promised high commissions or high returns such as doubling of money in short span of time. The advertisements / SMS messages usually contain a link, which directly prompts for a chat. Further, mobile applications, bulk SMS messages, SIM-box-based Virtual Private Network (VPNs), phishing websites, cloud services, virtual accounts in banks, Application Programming Interfaces (APIs) etc. are used to carry out financial frauds.

b) Keywords such as "Earn Online", Part Time Jobs" etc. are used by fraudsters to match their advertisements with the terms people are searching for. Such advertisements are displayed when the internet usage by Indian public is at peak. Majority of such fraudulent websites have domains – 'XYZ' and 'wixsite' and are redirected to messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.

c) Multiple Indian numbers are used for communicating with victims. Most of the times, the mobile number holders are found to be unaware about messaging platforms being operated in his/her name. In some cases, the mobile holders knowingly share the OTP in return for some money from the fraudsters.

d) The fraudster sends an investment link over chat. Each person has a referral code. Fraudster generally communicates in English and is found to be using Google Translate for communicating with victims.

e) First the victim's account is activated by seeking a screenshot over the messaging platform. Then a task is given to the victim to gain confidence of the person. Mandatory condition to perform the task is to load money through Payment Gateways (which are not authorized to operate in India). Call center is generally used to interact with the victims regarding the task. For instance, in case of failure to load funds, the call center executive initiates a call.

f) Once the task is complete, the victim is asked to withdraw the money through various payment aggregators.

g) Thus, on receiving the money, the victim gets lured into doing more tasks which again involves loading money. The process continues till a big amount is loaded when the fraudster stops responding to the victim.

h) Fraudsters keep the source code unchanged but keeps updating the UPI details daily and changes the investment websites and the domain.

i) Bank accounts are opened by 'money mules' using real / fake identities to receive stolen funds from compromised bank accounts. Fraudsters and their agents also source bank account holders offering them fixed rent or commission or lumpsum amount for using the account. Such accounts are used by fraudsters for transferring funds to hide their identity.

BEST PRACTICES AND RECOMMENDATIONS FOR REDUCING THE RISK OF DOWNLOADING HARMFUL APPS:

- Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store.
- Prior to downloading / installing apps on android devices (even from Google Play Store):
    - Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
    - Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
    - Do not check "Untrusted Sources" checkbox to install side loaded apps.
- Install Android updates and patches as and when available from Android device vendors.
- Do not browse un-trusted websites or follow un-trusted links and exercise caution while clicking on the link provided in any unsolicited emails and SMSs.
- Install and maintain updated anti-virus and antispyware software.
- Look for suspicious numbers that don't look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number. Genuine SMS messages received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field.

- Do extensive research before clicking on link provided in the message. There are many websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.
- Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organisation's website directly using search engines to ensure that the websites they visited are legitimate.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Exercise caution towards shortened URLs, such as those involving bit.ly and tinyurl. Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL. Users can also use the shortening service preview feature to see a preview of the full URL.
- Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information such as personal particulars or account login details.
- Customer should report any unusual activity in their account immediately to the respective bank with the relevant details for taking further appropriate actions.

Updated on 14-10-2022