CUSTOMER AWARENESS ON CYBER FRAUDS

Fraudulent phone calls and SMSs containing fraudulent URLs on the subject of KYC updation, linking of bank accounts, seeking confidential information of customers, are currently in circulation.

These are the attempts made by the fraudsters to siphon the money from the bank accounts of innocent people. Therefore, keep yourself safe from banking frauds and learn the tricks to avoid cyber frauds.

General tactics employed by fraudsters

- Fake helpline numbers on Google search
- Gift Parcel fraud/Drugs in Courier
- YouTube “likes” fraud
- Earn Online Task Fraud
- Part-time online Job Advertisement
- Work From Home –Movie ratings
- Insurance (Car, Life, health) renewal frauds
- Fake Websites/Discounts/Free Apps
- QR code scan fraud
- Update PAN/KYC
- Income Tax refunds
- Misuse of Aadhaar/Misuse of AEPS/BIOMETRIC
- Mistaken Payment Fraud

How to Safeguard Yourself

Password Usage Tips:

1. Never continue default passwords for any electronic devices/connections/Applications/Apps
2. Never store the passwords in the system or allow the system to remember
3. Do not use personal information such as own name, short form of own name, own initials, names of family, friends, co-workers, company or popular characters in USER IDs.
4. Never share Your or Bank’s passwords with anybody else. Banks never ask for your passwords

Password Construction Tips:

1. Passwords shall be at least 8 characters long, with numeric, upper case, lower case, and special characters like ~, @, #, $, %, &, wherever allowed.
2. Do not use personal information like date-of-birth, address, telephone numbers etc.
3. Do not use common words found in English dictionary.
4. Do not use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

Website/Mail usage safety Tips:

Thumb Rule: Stop-Verify-Click & Never transfer funds to unknown persons or entities in anticipation of high returns

1. Never Click on Links sent through Email / SMS
2. Do not respond to Email/SMS where the Sender doesn't address you by name.
3. Competitions and lotteries do not require you to pay an advance fee to collect winnings.
4. Never click/use unknown websites offering freebies/Discounts
5. Verify the https:// and correct name of the organization in the address i.e URL
6. Verify the Lock symbol in the URL before you give any information
7. Never open mails from unknown sources
8. Never click on the attachments of mails from unknown or known suspicious mails
9. Never click on the links given in the SMS offering jobs, gifts etc
10. Never respond to fake email notices stating that bills are pending, refunds are pending etc.

Best Practices for Users to remain safe

1. Always perform online financial transactions from a secure computer system updated with latest security updates/patches, anti-virus and antispyware software and personal firewall.
2. While making online transactions with credit/debit card, user must use his/her card only at established and reputed sites as there are less chances of card fraud on a reliable website.

3. Always ensure that the address of the website, where transactions are to be done, starts with "https://" and not "http://".
4. Change your card PIN (Personal Identification Number) periodically.
5. Do not disclose any personal information online like your date of birth, billing address, etc., on the Internet because that can be misused in order to unlock your account password.
6. Never share card details over phone or with anyone in person as it is easier way for others to get access to your confidential card information and make the online transactions.
7. Avoid sending card and account details through e-mail to prevent from malicious use by others.
8. Regularly check account statement related to the card and notify the card issuer Bank in case of any discrepancy.
9. Ensure whether your card is enabled/disabled for International use; Disable if it is not necessary. Check with your bank for any additional options such as restricting the usage of cards on different payment channels viz., PoS/ATM/e-Commerce or Domestic/International usage time-to-time through bank's own interface/app.
10. Report any loss due to cyber frauds to the Number 1930.