केनरा बैंक Canara Bank

EDUCATIVE SERIES

ON

Technology Banking Frauds

FOR CUSTOMERS

✓ *General standards and guidelines*

✓ *Precautions for staying safe*

Standard guidelines and safety precautions to be taken against fraudulent transactions - Banking

Mobile Banking/ UPI

○ *General Guidelines*

- ✓ *Always use password/ bio metric to protect the mobile phone.*

- ✓ *Always download the Mobile Banking App from the trusted source (Google Play Store/ Apple Store). Never trust any APK files from unknown sources.*

- ✓ *Choose a strong password for the Banking App to keep bank accounts and data safe.*

- ✓ *Review account statements frequently to check for any unauthorized transactions.*

- ✓ *Change PIN frequently and never share it with any one.*

- ✓ *Use "Card Less Cash" option to avoid/ minimize the usage of ATM card.*

- ✓ *Report the lost or stolen phone immediately to a service provider and block the SIM card.*

- ✓ *Monitor transactions regularly and bring any fraudulent transaction to the notice of the Bank.*

- ✓ *While exchanging, selling, lending or giving the phone for repair please make sure that the Banking App is uninstalled and temporary files, browsing history and cache got cleared.*

- ✓ *Always remember, to receive money there is no need to enter your PIN/ password anywhere.*

○ *Staying safe*

- ✗ *Never share PIN or confidential information over the phone or internet. Never share these details with anyone, including 'Bank Staff'.*

- ✗ *Don't click on links in emails/ social networking sites claiming to be from the Bank.*

- ✗ *Don't store sensitive information such as credit card detail, mobile banking password and user ID on the mobile phone.*

- ✗ *Inform the bank about changes in your mobile number to ensure that SMS notifications are not sent to someone else.*

- ✗ *Be cautious with offers from caller tunes or dial tunes or email attachments from known/ unknown sources.*

- ✗ *Be cautious while using Bluetooth in public places as someone may access your confidential data/ information.*

- ✗ *Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.*

- ✗ *Be careful about the websites while browsing, if it does not look authentic, do not download anything from it.*

- ✗ *Do not leave the smartphone unattended.*

- ✗ *Do not share confidential information via SMS/ WhatsApp or any other means.*

- ✗ *Do not use a public or unsecured Wi-Fi to login or transact with a Banking App.*

- ✗ *Do not force close the Mobile Banking App during an active session, instead, logout and then close the app.*

- ✗ *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.*

- ✗ Don’t click any unknown link in the Mobile (Fraudsters may access your device through phone sharing).

- ✗ Apps like Any Desk & etc. (Remote Access Apps) should not be installed in the mobile.

Internet Banking

○ *General Guidelines*

- ✓ *Make net banking passwords difficult to guess, change them regularly. Also, never share them with anyone, meaning just anyone.*

- ✓ *Before keying in sensitive information, ensure the site is running in a secure mode by looking for the padlock symbol at the bottom of the browser.*

- ✓ *Scan email attachments for viruses before opening them. When unsure about the source of an attachment, delete it. Also, ensure to install a good anti-virus system on the PCs and ensure that it is updated regularly.*

- ✓ *Keep Software Updated: One should keep their computer up-to-date with the latest security patches. This helps protect against known vulnerabilities that cybercriminals may exploit.*

- ✓ *Make it a habit of clearing browser history after confidential activities/ transactions.*

○ *Staying safe*

- ✗ *Don't access bank website from a link provided in an email from any source. Instead, type the address of the bank website in the address bar of browser to access the bank account. Don't click on any link provided in emails, they may redirect users to a fake/phishing site.*

- ✗ *Don't share the password or CVV details orally with banks. Bank never asks for confidential information like user ID, password, credit card number, CVV, etc., via mail, SMS or bank initiated phone calls.*

- ✗ *Never write down user ID, password on piece of paper, documents or phones for easy retrieval.*

- ✗ *Never use the "remember password" feature provided by browsers to save their net banking passwords.*

- ✗ *Don't access Net banking from cyber cafes. If accessed, please use the virtual key board to key in details and ensure to log out of the system once it is done.*

- ✗ *Do not use a public or unsecured Wi-Fi to login or transact with Internet Banking.*

ATM/ Debit Cards

○ *General Guidelines*

- ✓ *Conduct the ATM transactions in complete privacy.*
- ✓ *First use of the card must be on an ATM, else it will not be accepted at Point of Sale (POS).*
- ✓ *Ensure the current mobile number is registered with the bank so that it can get alerts for all the transactions.*

- ✓ *Always shield the ATM keypad from onlooker by covering the keypad while entering the PIN.*
- ✓ *Store the Debit card carefully so that the EMV chip does not get damaged.*
- ✓ *Ensure to collect the Debit card, after completion of the transaction.*
- ✓ *Please ensure that the card is swiped in your presence at POS terminal (Point of Sale).*
- ✓ *After completion of your transaction and before leaving the premises please ensure that "Welcome Screen" is displayed in the ATM/ Cash deposit machine (CDM).*
- ✓ *If cash is not dispensed and ATM does not display "cash out"/ "Unable to dispense cash", please report to the Bank Branch on the number mentioned in the official website of the Bank.*
- ✓ *In case of any discrepancy or failed transaction, immediately contact where your account is maintained.*
- ✓ *Beware of suspicious movements of people around the ATM or strangers trying to engage you in conversation or in any suspicious transactions.*
- ✓ *Look for extra devices attached to the ATMs that looks suspicious.*
- ✓ *Immediately check your phone for SMS for debit amount.*
- ✓ *Change PIN frequently and never share it with any one*
- ✓ *Do check if the card given to you by the merchant after completion of the POS transaction is your card.*

○ *Staying safe*

- *Do not write your PIN on the card or card wallet or do not store pin in your mobile.*
- *Do not keep your card and PIN together.*
- *Never lend your Debit card to anyone.*
- *Beware of “Shoulder Surfing” and ensure the transactions are carried on complete privacy manner.*
- *Never seek help from anybody by handing over the Debit card and revealing the PIN.*
- *Never accept assistance or offer from strangers at the ATM.*

- *Do not share your card or PIN details with anyone or in response to any phone calls / email/ SMS.*
- *Do not disclose your PIN to anyone, including bank employees and family members.*
- *Never leave your Debit card in the ATM/ CDM.*
- *Never leave your ATM transaction unattended. Step away only when the transaction is complete and the ATM returns to the Welcome Screen.*
- *Do not allow the card to go out of your sight when you are making a payment.*
- *Do not ignore SMS alerts regarding balance enquiry or mini-statement when the request is not initiated by them.*

Credit Cards

○ *General Guidelines*

- ✓ *First use of the card must be on an ATM for change/ generate PIN, else it will not be accepted at Point of Sale (POS).*

- ✓ *Ensure the current mobile number is registered with the bank so that it can get alerts for all the transactions.*

- ✓ *Store the Credit card carefully so that the EMV chip does not get damaged.*

- ✓ *Manage the card limits using Ai1 mobile banking app for additional safety.*

- ✓ *Please ensure that the card is swiped in your presence at POS terminal (Point of Sale).*

- ✓ *In case of any discrepancy or failed transaction, immediately contact where your account is maintained.*

- ✓ *Immediately check your phone for SMS for transaction amount.*

- ✓ *Do check if the card given to you by the merchant after completion of the POS transaction is your card.*

- ✓ *Use Bank ATM for Balance enquiry and change of PIN.*

- ✓ *Change PIN frequently and never share it with any one.*

- ✓ *Ensure updating of communication address in Bank records so that renewal card will be delivered by promptly.*

- ✓ *Regularly monitor transactions statements and bring any suspicious/ fraudulent transaction to the notice of the Bank*

- ✓ *Ensure updating of correct e-mail id with Bank for getting the monthly statement/ bill in time.*

○ *Staying safe*

- ✗ *Do not write your PIN on the card or card wallet or do not store it in mobile.*

- ✗ *Do not keep your card and PIN together.*

- ✗ *Never lend your Credit card to anyone.*

- *Never seek help from anybody by handing over the Credit card and revealing the PIN.*

- *Do not disclose your PIN to anyone, including bank employees and family members.*

- *Do not allow the card to go out of your sight when you are making a payment.*

- *Do not share your card or PIN details with anyone or in response to any phone calls/ email/ SMS.*

- *Don't share the password or CVV details orally with banks. Bank never asks for confidential information like credit card number, CVV, etc., via mail, SMS or bank initiated phone calls.*

- *Don't fall prey to any offer from unknown sources for the redemption of reward points.*

E Mails

○ *General Guidelines*

- ✓ *Be cautious about opening any attachments or downloading files you receive regardless of who sent them.*
- ✓ *Look for the sender email ID before you enter/ give away any personal information.*
- ✓ *Use antivirus, antispyware and firewall software and ensure to update them regularly.*
- ✓ *Always ensure to keep update with the web browser.*
- ✓ *Scan the attachments before opening with your scanner. It will detect and block potentially harmful files and reduce the risk of infecting your system and network.*

- ✓ *If you receive any suspicious e-mail, do call the Bank to confirm if it is legitimate or not.*
- ✓ *Do use a separate email accounts for things like shopping online, personal etc.*

○ *Staying safe*

- ✗ *Do not reply to an e-mail or pop-up message that asks for personal or financial information.*
- ✗ *Do not e-mail personal or financial information i.e. Credit Card or other sensitive information via email.*
- ✗ *Never click on any email or social media messages you do not expect or need.*
- ✗ *Do not open e-mail that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try another means.*

- ✗ *Never open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.*

- ✗ *Avoid using your company e-mail address for personal communications.*
- ✗ *Do not open any spam e-mail.*

Passwords

General Guidelines

- ✓ *Length of password should be 8 to 12 characters.*

- ✓ *Password should be combining with unrelated words.*
- ✓ *Use an entire phrase and change some of the letters to special letters and numbers.*
- ✓ *Use a combination of upper and lower case letters, symbols and numbers.*
- ✓ *The longer your password, the stronger it is.*
- ✓ *Use different passwords for every account.*
- ✓ *Ensure to set new password significantly different from the previous passwords.*

Staying safe

- ✗ *Never share the password with anyone.*
- ✗ *Don't use personal information in your password.*

- ✗ *Don't write down your password or store it in an unprotected app on any device.*
- ✗ *Avoid using 123456, the most common of all passwords.*
- ✗ *Switching a letter to a symbol like p@ssw0rd too is an obvious trick that hackers know. Password cracking programs contain every type of these combinations in every language.*
- ✗ *Avoid using names of your favorite name, sports team, person, etc.*
- ✗ *Avoid using single words and adding a number or punctuation at the end.*
- ✗ *Avoid using common patterns like 111111, abc123 or 654321.*

Ways to Block / Hot list the Digital Products :-

Product	Blocking / Hot listing options			
	SMS/WHATSAPP	**Mobile Banking**	**Internet Banking**	**Toll Free Number**
Credit Card	Whatsapp banking (9076030001)- All Services> Card Services> Credit Card Services>Block Credit Card	Canara ai1 app>> Manage Credit Card>>Block/Unblock Card	Internet Banking>>Cards>>Manage Credit Cards>>Block/Hotlist Card	1800 1030
Debit Card	Whatsapp banking (9076030001)- All Services> Card Services >Debit Card Services> Block Debit Card	Canara ai1 app>> Manage Debit Card>>Block/Unblock Card	Internet Banking>>Cards>>Manage Debit Cards>>Block/Hotlist Card	1800 1030
Mobile Banking	-	-	Internet Banking>>Other Services>>Block /UnBlock Mobile Banking	1800 1030
Internet Banking	‘LOCKIBU USERID' TO 9010982223 from registered mobile number	Canara ai1 app>>Other Services>>Block/Unblock IB	-	1800 1030
UPI	UPI users can send SMS “BLOCKUPI” to 9901771222 from registered mobile number to block the UPI services.	i. Pre-login screen: “Block UPI” option is available in pre-login screen of Canara ai1 app under More>>Block/Unblock. ii. Post login: - User can block the UPI service post log in to the Canara ai1 app; Profile>>UPI>>UPI Services (toggle button).	Internet Banking>>Other Services>>Block / UnBlock UPI	1800 1030
AEPS	SMS 'BLOCKAEPS' to 7799719408 from registered mobile number Whatsapp banking (9076030001)- All Services> Banking Services> Enable/Disable AEPS	-	Internet Banking>> Other services >> Enabling/disabling AEPS	1800 1030

केनरा बैंक Canara Bank