Safe Banking Tips

A. Mobile Banking - Safety Tips

- Set up a Pin/password to access the handset menu on your mobile phone.
- Register/ update your mobile number and e-mail ID for alerts to keep track of your banking transactions.
- While installing the application only give the minimum required permission to applications.
- Do not install the mobile application shared in url links and mail, only install the application from the authorized play/app store.
- Do not follow any URL in message that you are not sure about.
- Never leave your mobile phone unattended.
- Log out from online mobile banking/UPI application as soon as you have completed your transactions.
- Avoid using unsecured Wi-Fi, public or shared networks.
-

Tips for safe and secure UPI/Mobile Banking transactions:

- Ensure app is downloaded from trusted sources. Just because the name of an app resembles the name of the bank, don't assume it is the official Punjab & Maharashtra co-operative Bank app. It could be a fraudulent app designed to trick users into believing the service is legitimate.
- Do not modify mobile phone core configuration which is technically called as jailbreaking or rooting of the device. It will make your mobile phone susceptible to an infection from a virus, Trojan, or malware.
- Be alert to changes in your mobile phone performance. If you download any new applications and your mobile phone starts performing differently (for example-responding slowly to commands or draining its battery faster), that could be a sign that malicious code is present on your mobile phone.
- Monitor your financial records and accounts on a regular basis. Use the electronic account alerts to send to your email or mobile device on account activity. Regularly review your statements with online banking. This will enable you to spot any suspicious activity.
- Punjab & Maharashtra co-operative Bank will never ask for your password under any circumstances. Do not tell your password to others under any circumstances (including mobile phone support operators or mobile phone sales representatives etc.). Fraudsters will try to obtain mobile banking passwords by e-mail, letter, phone calls,

asking for your mobile banking account number, username, password, and other important information. If you have any doubts, please contact Punjab & Maharashtra co-operative Bank customer care 1800 22 3993.

- Use strong passwords that are difficult to crack.
- Be aware of shoulder surfers. Be extra careful while typing confidential information such as your account details and password on your mobile in public places.
- It is good practice to change your mobile banking password regularly.
- Do not lend others your phone with the mobile banking function opened as this will prevent infringement and deter others from spying on your personal information.
- Don’t use your device in an unsecured Wi-Fi network or in a public place.
- Don’t send account numbers or other sensitive information through regular e-mails or text messages because those are not necessarily secure.
- Password protect your mobile device and lock your device when it’s not in use. Keep your mobile device in a safe location.
- Delete text messages from your financial institution on your mobile device, especially if they contain sensitive information.
- If you change your mobile number, immediately contact Punjab & Maharashtra co-operative Bank to change the details of your mobile banking profile. You should also take additional precautions in case your device is lost or stolen.

B. ATM Safety Tips:

Precautions while using an ATM

- Memorise your PIN. Do not write it down anywhere, and certainly never on the card itself.
- Your card is for your own personal use. Do not share your PIN or card with anyone, not even your friends or family.
- "Shoulder surfer" can peep at your PIN as you enter it. So stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN.
- Do not take help from strangers for using the ATM card or handling your cash.
- Press the 'Cancel' key before moving away from the ATM. Remember to take your card and transaction slip with you.
- If you take transaction slip, shred it immediately after use.

- Please ensure to BLOCK your ATM/debit card instantly in case of loss / theft / misuse, by any of the below mentioned services or by visiting nearest Branch.

Services	Sent to
SMS Banking facility	HOT(SPACE)< LAST FOUR DIGIT OF ACCOUNT NUMBER> sent on 9773251313
Missed Call Facility	9278882010
Call Center- Toll Free Number	1800223993
You can also hotmark your Debit card using PMC Bank Mobile Banking App	

- Register your email id and mobile number or update new/changed mobile number with the Bank to get regular transaction alerts / updates.

Skimming

Skimming is an act of stealing information through the magnetic strip on the cards that are used in ATMs and merchant establishments. Fraudsters collect information from a credit/debit/ATM card by reading the magnetic strip on the reverse of the card. For doing this, they conceal a small device in the card slot of ATM's or merchant payment terminals. This 'skimmer' scans the card details and stores its information. A tiny strategically positioned camera may also be used to capture the PIN. Skimming can occur in ATMs, restaurants, shops or other locations.

Tips to Protect Yourself From Skimming

- Protect your PIN by standing close to the ATM and shielding or cover the key pad with your other hand when entering your PIN.
- If you see anything unusual, strange, suspicious, something that does not look right with the ATM or if the keypad does not feel securely attached, stop your transaction and inform the bank.
- If it appears to have anything stuck onto the card slot or key pad, do not use it. Cancel the transaction and walk away. Never try to remove suspicious devices.

- Be cautious if strangers offer to help you at an ATM, even if your card is stuck or you are having difficulties. Do not allow anyone to distract you
- Keep your PIN a secret. Never reveal it to anyone, even to someone who claims to be calling from your bank or a police officer.
- Check that other people in the queue are at reasonable distance away from you.
- Regularly check your account balance and bank statements, and report any discrepancies to your bank immediately.

C. Internet Banking- Safety Tips

Phishing

Phishing is an act of sending a fraudulent email and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site. The fraudster lures victim purporting to be from banks website for capturing customer's sensitive personal information like user-id, password or PIN, date of birth, CVV number etc.

Tips To Protect Yourself From Phishing

- Do not open spam mails. Be especially cautious of e-mails received from unrecognized senders.

    - Ask you to confirm personal or financial information over the Internet and/or make urgent requests for this information.
    - Try to upset you into acting quickly by threatening you with frightening information.

- Do not click on links, download files or open attachments in e-mails from unknown senders. Be cautious even if the e-mail appears to come from an enterprise you do business with. It is a good practice to call up the concerned to confirm in case the e-mail is unexpected.
- Communicate personal information only via secure web sites. In fact:

    - When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".
    - Also, check if the website address is correct before conducting online transactions.

- Protect your computer by installing effective anti-virus / anti-spyware / personal firewall on your computer / mobile phone and update it regularly.
- Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.
- Do not disclose details like passwords, debit card grid values, etc. to anyone, even if they claim to be bank employees or on e-mails/links from government bodies like RBI, I.T. Dept., etc
- Type the web address in the browser. Do not use links received in e-mails.
- In case you have used a cyber cafe / shared computer, change your passwords from your own computer.
- Register for e-mail and mobile alerts to check your account regularly.
- Report any fraudulent incident to the Bank / institution on the number mentioned on the Debit / Credit card, bank / credit card statement or official website.
- Do not rely on the name and source in the "From" field of the email address as it may be easily manipulated by the fraudster to a valid email account of bank.
- Always access your bank website by typing the URL in the address bar of your browser only.
- Always check the authenticity of the software before downloading.
- If you get an email asking for personal or credit/debit card information, please do not provide this information no matter how 'genuine' the page appears to be. Such pop-ups are most likely the result of malware infecting your computer. Please take immediate steps to disinfect your device.
- Any bank or their representative will never send you emails to get your personal information, password or one time SMS (high security) password. Such e-mails are an attempt to fraudulently withdraw money from your account through Internet Banking.

Vishing

Vishing is an attempt of a fraudster to take confidential details from you over a phone call. Details like user id, login & transaction password, OTP (One time password), URN (Unique registration number), Card PIN, Grid card values, CVV or any personal parameters such as date of birth, mother's maiden name. Fraudsters claim to represent banks and attempt to trick customers into providing their personal and financial details over the phone. These details will then be used to conduct fraudulent activities on your account without your permission leading to financial loss.

Tips to Protect Yourself from Vishing

- Your bank would have knowledge of some of your personal details. Be suspicious of any caller who appears to be ignorant of basic personal details like first and last name (although it is unsafe to rely on this alone as a sign that the call is legitimate). If you receive such a call, report it to your bank.
- Do not call and leave any personal or account details on any telephone system that you are directed to by a telephone message or from a telephone number provided in a phone message, an e-mail or an SMS especially if it is regarding possible security issues with your credit card or bank account.
- When a telephone number is given, you should first call the phone number on the back of your credit card or on your bank statement to verify whether the given number actually belongs to the bank.
- If you get an SMS or call asking for personal or credit/debit card information, please do not provide this information.

A new modus of operandi for fraudulent transactions in UPI application has been observed, through which fraudster can easily take remote access of a victim's mobile device and carry out transactions.

Details are as under:

- Fraudster would attract the victim on some reason to download an app called 'AnyDesk' from Playstore or Appstore. It may be noted that, there are more apps similar to 'AnyDesk' that help provide remote access of device to other users.
- The app code (9 digit number) would be generated on victim's device which the fraudster would ask the victim to share.
- Once fraudster inserts this app code (9 digit number) on his device, he would ask the victim to grant certain permissions which are similar to what are required while using other apps.
- Post this, fraudster will gain access to victim's device.
- Further the mobile app credential is vished from the customer and the fraudster then can carry out transactions through the mobile app already installed on the customer's device.

Above modus operandi can be used to carry out transactions through any Mobile Banking and Payment related Apps (including UPI, wallets etc.)

In this connection, we request you to guide our customers to take adequate care while installing the unknown/not trusted applications in your online transaction devices.