Bank AL Habib Limited
بینک الحبیب لمیٹڈ

Secure Online Banking

DON'T SHARE YOUR PRIVATE INFORMATION ONLINE

Bank AL Habib will **NEVER** contact you via Phone, SMS, E-mail or any other means asking for your Personal Information, Netbanking or AL Habib Mobile App Username, Password, Debit/Credit card number, PIN, OTP or CVV.

BE CAREFUL WHERE YOU GO ONLINE

Avoid using Netbanking while connected to an unknown Wi-Fi especially for financial transactions at internet cafés, libraries, or any other public sites to minimize the risk of information being copied and abused after you leave.

ALWAYS LOG OFF

Remember to log off from your Netbanking platform and close your browser window/tab, when you are finished with your online banking session to ensure the closure of your active Netbanking session with Bank AL Habib.

DIFFERENTIATE BETWEEN SECURE AND INSECURE COMMUNICATION

Ensure that the website you are accessing has a lock sign in the address bar of your browser and the URL contains 'HTTPS' and not 'HTTP' i.e. 'https://www.website.com'. It will enable the communication with the website on a secure channel.

UPDATE YOUR CONTACT DETAILS

Customers are advised to update their primary contact details such as registered mobile number and email address with the Bank with the Bank to receive emails and SMS alerts for account login / logout and transaction activity. Any suspicious activity noted should be reported immediately on the Bank AL Habib helpline:
(+92 21) 111-014-014.

Advice on Device Security

INSTALL AND UPDATE AN ANTI-VIRUS SOFTWARE ON YOUR DEVICES

Always use an anti-virus software on your device. To remain effective, the software should be updated regularly with the latest virus definitions. Never open an e-mail attachment that contains a downloadable suspicious file as they may contain viruses.

PROTECT YOUR DEVICES

- If you stop receiving calls or texts, and you don't know why, check in with your mobile operator immediately.
- Protect your device with a secure authentication method to prevent unauthorized access if it is left unattended or stolen. (Fingerprint or Face Recognition authentication is preferred)
- Use the official application store i.e. App Store and Google Play for Apple and Android based devices respectively to download AL Habib Mobile Application i.e AL Habib Mobile

- Do not store passwords or account numbers on your mobile phone.
- Never use a jailbroken or rooted device for your mobile banking.
- Ensure that all your devices are updated with the latest available operating system version.
- Do not install mobile applications from any untrusted source. Always install apps from Google Play / App Store.
- Install an antivirus on your mobile device to avoid viruses / malwares attacks.
- Factory Reset your mobile device before selling.
- Never leave your AL Habib Mobile App running in the background, log out once you are done using it.

Password Guidelines

All users should conform to the following guidelines for password composition:

- The Password shall be UNIQUE with a minimum of 8 characters and a maximum of 12 characters long.
- Passwords shall be a **combination of alphabets both upper and lower-case** (e.g., a-z, A-Z), **numeric and special characters** (e.g., 0-9, @#$^& () _+|~-=`{}()[]:";')
- **Avoid use of Dictionary words** as they are easy to predict.
- Passwords should **not be a word in any language, slang, dialect, jargon,** etc.
- Password should **not contain your username**
- Regularly **change your Netbanking password**
- Netbanking **password must be different from Social Media Accounts password**