Al Mubasher Retail Internet Banking Privacy Policy

Introduction

Al Rajhi Bank acknowledges your rights to the privacy of any personal information you may provide to the bank while performing your Internet banking transactions. Al Rajhi Bank is committed to providing a high level of security and privacy for any information involving the use of our retail Internet banking services. The bank guarantees any transaction conducted through Internet banking and any personal or financial information exchanged by such means are processed in a HTTPS (secure) encrypted method which complies with industry security standards.

Exchange & Storage of Customer Information

Registration

In order to protect your personal and financial information Al Rajhi Bank requires you to register to the service and specify your preferred User ID and Password. The registration process requires 2 factor authentication acquiring your ATM Card number, ATM PIN and account number. Similarly in order to login to our Internet banking you need to specify your user name and password. Any personal information collected by the Bank is used solely for the purposes of providing you with banking services.

Transfer of Information

Al Rajhi Bank maintains the confidentiality and integrity of the information it holds for you and the exchange of the information is performed in a secure manner. Your personal and financial information is not shared with any third party, except where, the information is required in order to meet your instructions. When such disclosure is required by, or allowed by, law, governmental or regulatory bodies due to fraud investigation or audit. Or when you yourself request or permit disclosure of such information in written.

Information Access by Bank employees

Bank employees access to your personal and financial information is limited and is only provided such that those employees can provide you with the services that you require. The bank continues to review, develop and protect all our resources with the best security and controls available and known to the banking industry. No Bank employee will ever ask you for your internet banking user ID and password, your ATM card number and its PIN, nor should you ever provide it to anyone in any context or for any reason. Al Rajhi Bank do not ever want you to disclose your password or PIN number to any bank employee or any individual.

Security

Al-Rajhi Bank strives to maintain best security standards to prevent any unauthorized access to your confidential information. Security measures used include intrusion detecting/prevention systems, virus detecting systems, data encryption, and firewalls. Al Rajhi Bank takes all necessary steps to protect customer's personal information, including accounts, transactions, user names and passwords during the information exchange between you and the Bank.

User Name and Password
Access to your Internet banking is protected with user names and passwords which are known only to you. Your password must be used only by you when you access your accounts and when you request, that transactions be executed on your behalf. You must safeguard your user name and password and ensure that your ATM card and its PIN number is safe with you. In case the your ATM card number, ATM PIN, User name and Password for Al Mubasher Retail is compromised you must take the necessary steps to change them or notify the bank immediately to protect your self from any financial loss. You may contact Al Rajhi Bank by calling its call center or by visiting the nearest branch.

Access to Information
Access to Internet banking allows you complete access to all current accounts, credit cards, investments, Mobile banking alerts and various other important personal and financial information.

How to identify a secure access
While using our Internet banking you will see a pad lock sign appearing in your browser and HTTPS appearing in the beginning of the address bar (URL) which means you are connected to a secure website. If you do not see the above mentioned marks appearing in your browser you must not provide any confidential personal or financial information to that website and report the matter to the bank for further assistance.

Delegating the authority to use Al Mubasher Retail
Al Rajhi Bank is entitled to act on any instruction in terms of a transaction or inquiry it receives using your User name and password. If you share your user ID, Password, ATM card number and PIN number with another person you are authorizing that person to use our Internet banking services. In such a case you will bear full responsibility for all transactions performed using your user name and password, even if you did not intend or authorize the nominee to act as you.

Secure Transactions
Some of the transactions in Internet banking require the use of One Time Password which is an additional security measure implemented to safe guard high risk transactions. This security measure requires you to provide your mobile number in any Al Rajhi Bank ATM machine as the bank sends a transactional password to your mobile via SMS. You are required to provide your mobile number with care and never insert the mobile number of any other individual or mobile which is not or does not remain in your possession.

Inactive Sessions
Our Internet banking will automatically log you out after a certain specified period if you are inactive while logged in to the service. This is to reduce the risk of someone else accessing your account if you leave your computer unattended. Al Rajhi Bank however strongly recommends that you use the logout function of the site as soon as you finish your Internet banking session and close the browser for maximum safety.

Cautions & Protection Measures

Protecting Personal Information
Never share your ATM Card Number, ATM PIN with anyone or note it down on any paper, PC, mobile phone or any other storage device which could be lost or compromised. It is recommended that you remember your ATM PIN and never write it anywhere specially on the back of your ATM Card or in your wallet.

Password Protection measures
Never share your internet banking user ID and password with anyone and never save it or note it down on a paper or PC. Al Rajhi Bank advises all customers to remember their user names and passwords and change them periodically.

Operating system, browser and software updates
Keep up to date with software fixes (also known as 'patches' or 'security updates'). Using a current browser will maximize your security. Al Rajhi Bank also advises you to use licensed software and update it periodically as and when required.

Anti-virus protection
Ensure that your computer has an up-to-date anti-virus protection program to detect and remove viruses. Also consider SPAM email filtering. The Bank is not responsible for any virus or other malicious code that you may encounter using internet. Al Rajhi Bank encourages you to routinely scan your computer, e-mails and storage using industry recommended and recognized virus protection products.

Anti-spy ware protection
Use a current anti-spy ware protection program to detect and remove spy ware from your computer.

Firewall
Use a firewall to prevent unauthorised users from gaining access to your computer or network.

Keeping an eye
Al Rajhi Bank advises all customers to check their previous login status appearing on the welcome page. This allows you to identify if there was an attempt to login to your account from a fraudster.

Be Extra Careful
Al Rajhi Bank does not recommend usage of public place Internet facilities due to greater chance of your sensitive information being compromised. However, if you do, Al Rajhi Bank suggests that whenever you are accessing Internet banking from a public or shared computer such as those at Internet cafes, libraries, airports, hotels, etc. please adhere to the following precautions;

1. Ensure no one standing behind you is looking over your shoulder while accessing our site.
2. Logout of the site as soon as you finish your Internet banking session.
3. Close the browser by clicking on the 'X' icon, usually located at the top right-hand corner of the screen.
4. Verify that the last logon time corresponds with your last Internet banking session when you next logon to the site.
5. Change your password or access code as soon as possible when you next logon at a trusted secure computer.
6. Never download or save your account statements or relevant information on a public PC.

Hoax emails and Phishing sites

Fraudsters have been known to set up copies of banking sites with the purpose of capturing personal online banking logon details. They then send out an email that instructs the recipient to visit the website and logon in order to verify details. Unfortunately, when people enter their details into these sites the information is recorded and the fraudsters use it to transfer funds out of the real online banking facilities.
These websites and emails will often look legitimate so being able to identify a fake email from a real one can be a little difficult. Here are some things to consider:
1. These emails may be headed 'Dear Al Rajhi Bank Customer'. We know who you are so we'll always greet you personally, while fraudsters are unlikely to know your name. Members are advised not to click on any links, open attachments or enter any personal information.
2. The message is in no way associated with Al Rajhi Bank. Al Rajhi Bank has a policy to never solicit security information via email or ask members to follow Internet links. Al Rajhi Bank will never send you emails asking for your Internet banking security details.
3. Customers should only access Al Rajhi Bank's Internet banking site by typing the website address www.alrajhibank.com.jo into the address bar on their browser and then pointing to Al Mubasher Retail Internet banking. Customers can access Al Mubasher Retail directly by specifying the following URL in the browser https://www.almubasher.com.sa
4. When ever you suspect that an email or a website requires you to provide your important financial or personal information always verify that the URL in the address bar appears as http://www.alrajhimubasher.com.jo/ and a pad lock sign appears at the bottom of your browser.
Please disregard any email that advises you to access our site and provide any of your personal details. Instead, report the email to Al Rajhi Bank by calling our call center number and then delete it immediately.