Online Security Overview

Safety Is Our Focus

Al Rajhi Bank is committed to making sure that your online information is always safe and secure. With Al Rajhi Bank state-of-the-art security infrastructure in place, as well as the security built into your own browser, we are confident that your online information is private and secure from prying eyes.

Your Responsibility

While Al Rajhi Bank does everything it can to protect the confidentiality of your online information, we can't do it alone. Just as in the real world, where you take steps to protect your financial information, you will need to take ownership of your online safety. Here are some keys steps to protecting yourself while using Al Rajhi Bank online services via the Internet:

The 5 Steps to Online Security

1. NEVER reveal your Al Rajhi Bank Online services password or ID (Identification) to anyone - ever! Your password and ID are designed to protect the privacy of your banking information, but they only can work if you keep them secret. Attempts to break these passwords are monitored by special software, which will only allow a few attempts before the password needs to be reset. If you think your online password or ID has been compromised, change it immediately!
2. Don't leave your PC while you are in the midst of using any of the online services provided by Al Rajhi Bank
3. When you are finished using Al Rajhi Bank Online Services, be sure to LOGOUT the secured pages. This will automatically log out your session.
4. If other people have access to your computer, clear your browser's cache in order to remove copies of web pages that may have been stored temporarily on your system, browsers have the ability to cache information, that is, to remember a page or an image from a website. This makes Internet surfing quicker because when you return to a Web page previously visited, the browser can present a stored page without having to request the page from the server again. Refer to your browser's Help file for instructions on clearing your cache.
5. If you send Al Rajhi Bank an email remember not to include private information regarding your accounts or yourself. Others can potentially read email sent via the Internet in transit.

Tips for creating a secure password

1. Mix capital and lowercase letters.
2. Mix alphabets and numbers. (e.g omega3ruh1)
3. Create a unique acronym.
4. Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh'

Things to avoid

1. Don't use a password that is listed as an example of how to pick a good password.
2. Don't use a password that contains personal information (name, birth date, etc.)
3. Don't use words or acronyms that can be found in a dictionary.
4. Don't use keyboard patterns (asdf) or sequential numbers (1234).
5. Don't make your password all numbers, uppercase letters or lowercase letters.
6. Don't use repeating characters (aa11).

Tips for keeping your password secure

1. Never tell your password to anyone (this includes significant others, roommates, parrots, etc.).
2. Never write your password down.
3. Never send your password by email.
4. Periodically test your current password and change it to a new one.

Your Browser's Security

All Al Rajhi Bank Online Services use 128-bit SSL strong encryption during your online sessions to safeguard your data. Encryption essentially is a sophisticated way of scrambling your online information before it leaves your computer, so that if intercepted it is completely unreadable. We require that your web browser support 128-bit encryption because it is approximately 300 times stronger than 40-bit encryption. While 40-bit encryption might be fine for low-risk transactions, security professionals all agree that it is not adequate for protecting financial transactions. When you request information via Al Rajhi Bank Online on the Internet, your request is encrypted as it travels. We then decode your request for information and send it back to you, again - safely encrypted. When you receive it, your browser decodes the information and displays it.

You can identify that your online information is encrypted in Netscape if the small key or lock at the bottom left-hand corner of your screen is unbroken. Users of Microsoft browsers will see a lock appear during an encrypted session.

- We strongly recommend that you use the latest version of your preferred browser. The most up-to-date version of your preferred browser is normally available as a free download from the relevant browser manufacturer's website.
- The latest versions of browsers are more secure than older versions, which is particularly important when doing your banking via the Internet.

Most Windows based PCs are preinstalled with Microsoft Internet Explorer, therefore it is the most commonly used browser. Because of this, Internet Explorer is the browser most attacked by viruses and spy ware.

- If you use Internet Explorer it is particularly important to run a virus scanner and a spy ware scanner regularly and keep it updated with the latest security patches from Microsoft.

Identity Theft

Identify theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Fraudsters use information submitted via these fraudulent verification pages to use credit cards for unauthorized purchases, clear out bank accounts or sell the information to identity theft rings.

There are many ways and manners in which Identity theft can occur, but the two most common are set out below:

Phising is when a fraudster sends out messages (to email addresses obtained illegally), pretending to be from another company (e.g. the bank). The purpose of these emails is to extract your personal information, which can then be used by the fraudster to commit fraud in your name. Remember: Al Rajhi Bank will never ask for your username or password via email.

Spoofing is when a fraudster creates a website that looks like a genuine website, like the Al Rajhi Bank website, and also has a similar website address (URL). They then commit online fraud by urging people to transact on this fake website (e.g. deposit money, purchase goods). Remember: Al Rajhi Bank website address ishttps://www.almubasher.com.sa and no other company can duplicate this.</spoofing<>

What to look out for

Deceptive Subject Lines :

These look as if they are genuinely related to the company supposedly sending the e-mail.

Forged Sender's Address:

An easy deception method to make the e-mail appear as though it has come from the company it is claiming to be.

Genuine Looking Content :

They copy images and text styles of the real sites in order to fool the reader. Trusts and authentication marks are duplicated and they may even have genuine links to the company's privacy policy and other pages on the legitimate website to create an illusion of authenticity.

Disguised hyperlinks :
E-mails may display a genuine website address, but when you click on it, the hyperlink will take you to a different website. Look out for a long website address as it will take you to the site after the '@' symbol. Example:
http://www.genuine-site.com-name@fraud-site.com
If you clicked on this hyperlink it would take you to http://fraud-site.com as it is after the @ symbol.

Tips to protect you

1. Never submit your personal details i.e. account number, PIN, Password or Random Verification Number anywhere else than the official Al Rajhi Bank Internet Banking login page.
2. Activate Eshaar; Notification function for Internet banking users and get notified through SMS when there is activity on your Internet banking service anytime, day or night.
3. Never click on hyperlinks within e-mails as the hyperlink that you are linking to may be different to the one reflected in the e-mail. Hyperlinks within e-mail can easily be masked.
4. Use SPAM Filter Software to reduce the number of fraudulent and malicious e-mails you are exposed to.
5. Use Anti-Virus Software.
6. Use a Personal Firewall.
7. Keep Software Updated (operating systems and web browsers).
8. Always look for "https://" and padlock on web sites that require personal information. Although this does not guarantee that the site you are entering is a genuine site or that it is secure, the absence of these indicates that the web site is definitely not secure.
9. Keep your computer clean and free of Spy ware.
10. Educate yourself about fraudulent activity on the Internet.
11. Check and monitor your account statements periodically.

Al Rajhi Bank Other Security Features

We closely track each time you connect to Al Rajhi Bank and monitor the session to make sure that information sent back and forth is sent only to your PC. We have a "Firewall" in place which is a highly sophisticated piece of software and hardware that reviews messages coming in and out of Al Rajhi Bank - so that only authorized users are able to pass through to the banking system. Any messages that do not conform to extremely strict requirements are rejected and that online session is terminated. This type of technology is designed so that the most sophisticated hacker can't damage our site or access your private account information.
To help you ensure that you are really attached to Al Rajhi Bank during your online

sessions, we use digital identity verification. We have a digital server certificate from Verisign - the premier certification authority on the Internet. Your browser uses it each time you sign on to let you verify that you are connected to Al Rajhi Bank.
As you might guess, we have a number of other security procedures in place, which we can't disclose due to security reasons. These are designed so that our Internet partnership is a safe and secure one.