

To report or inquire please call us:

**+974 4425 4040**



## Traveling Security Tips

### General

- Memorize your PIN and e-banking passwords as they are personal information.
- Do not write your PIN or e-banking passwords down; especially not on the Bank card.
- Do not share your PIN and e-banking information with anyone. Masraf Al Rayan cannot be responsible of any issues resulting from you sharing your information.
- Do not forget your card after using it at the ATM or after paying at the merchant.
- Update your banking/personal information directly inside any of Masraf Al Rayan's Branches.
- Protect your PIN at all times, type it in by yourself, and make sure to hide it as you are keying it in.
- Call Masraf Al Rayan immediately if:
  - You lost your bank card.
  - You become aware of a transaction that you do not recognize or suspect that a transaction that you did not authorize occurred.
  - Your card has been captured by the ATM.
- It is preferred that you use an ATM that is in public clear sights.
- Make sure nobody is watching you while keying your PIN, stay alert of your surroundings.
- Do not use an ATM where the keypad or the card slot is not properly attached, or if it looks like a fake card slot, or if something appears to come out of it.
- Keep all receipts and transactions records with you.
- Wait as long as possible to withdraw your cash at the ATM, if you do not receive the money then call Masraf Al Rayan immediately while standing in front of the ATM.

### Before You Travel

- Check the limit of your Masraf Al Rayan's credit card and its expiry date.
- Make sure that you have the Bank's contact numbers before you travel and that the Bank has your up to date information.
- Take your mobile phone with you when you travel to receive transactions notifications.
- Make sure that all the information that is pre-written on your payment card is clear.
- Inform Masraf Al Rayan about your destination.

### While Traveling

- Keep your payment card safe, treat it as money.
- Make sure you are reachable by phone and or email so Masraf Al Rayan can contact you.
- Make sure that you are handling your card while paying or you are keeping it within your sight.
- Do not carry all your payment cards at the same time.
- Keep some money for emergencies.
- Avoid using your Cards for paying small amounts

**To report or inquire please call us any time at +974 4425 4040**

To report or inquire please call us:

**+974 4425 4040**

## **After You Travel**

- Change your online banking passwords regularly, and particularly after returning from travel.
- Review your Bank account transactions after your trip and compare with the payments and receipts kept during your holidays.
- If fraudulent transactions happen follow up on your return with Masraf Al Rayan immediately.

## **Be Careful While Making Online Purchases**

- Research the merchant before placing an order and always buy from reputable sellers stores and websites.
- Reliable companies should advertise their physical business address and at least one telephone number for customer service or for ordering products.
- Call the phone number and ask questions to determine if the business is legitimate.
- Make sure the website is reputable. If you are uncertain, order over the phone instead of online.
- Check for anything that looks unfamiliar, unprofessional, or out of place to you.
- Check the amount before placing the order, because of site spoofing.

## **Internet scamming**

- There are websites that appear professionally designed and legitimate, but that their purpose is collecting sensitive information from unsuspecting visitors. These websites can be detected by carefully checking the URL (the full website address details on your browser).
- Never respond to or open internet links or attachments in unsolicited emails.

## **Shop at secure Websites**

Shop at secure websites: A secure website uses encryption technology to transfer information from your computer to online merchant's computer system which keeps safe confidential information such as credit card details.

## **Learn about safe Internet Sites**

- Look for the text "**https://**" in the start of the website address or URL (before you enter your personal or private information; inclusive of credit card details).
- This means that the information is encrypted between your browser and the site you are purchasing from, which keeps it safe from prying eyes while it is transmitted across the internet.
- Do not allow websites to keep your credit card information.
- Make sure that there is a tiny closed padlock (locked) in the address bar, or on the lower right corner of the window.
- Always check for the browser "lock" icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate Web site.

## **System and Website Update**

- Keep your system and web browser software up to date: Make sure you install all the latest

**To report or inquire please call us any time at +974 4425 4040**

To report or inquire please call us:

**+974 4425 4040**

updates for your system and internet web browser software. Keeping your browser and operating system up to date will ensure that these settings are safeguarded and performing as well as possible.

- Install and keep up to date your security software (firewall, antivirus and anti-spyware software): It's important to install and keep this software up- to-date, and perform regular scans of your computer to help protect you from such threats as viruses, spyware, and spam and generally safeguard your personal information.
- A number of different providers produce complete security software packages. Review all packages available then assess which security software is best for you.
- Save all transaction details and regularly check your bank statements:
  - ✓ Print out or make note of the seller's identification, the item description and the time, date and price you paid or bid on the item.
  - ✓ Print and save copies of your order confirmation screen and all email communications.
  - ✓ Regularly check statements for any transactions that look suspicious. If any found, report it immediately to Masraf Al Rayan.
  - ✓ You can also request that your bank send **SMS** confirmations of online transactions. This will provide you with an early warning of any fraudulent activity.
- Use your personal computer and a private Wi-Fi for online shopping.
- Make sure that you logout from the shopping website after your are done; do not remain logged in.
- Do not disclose your online payment and shopping passwords. For example, PayPal account, MasterCard secure code, VISA's Verified by VISA, and online shopping account.
- When registering a name or password, avoid using a family member's name or your children's names etc. - use an alternative which cannot be easily guessed by fraudsters
- Use a strong password—at least eight characters, with a combination of numbers, letters (lower case and upper case), and punctuation symbols (or special characters).
- Don't use the same password for your banking that you use for any other online accounts.
- Keep your passwords safe—don't leave them in a file on your computer or in a sticky note on your monitor.
- Change your passwords periodically.

### **Phishing Spam Tips**

- **Phishing** is the act of obtaining information by pretending to be a legitimate source.
- Phishing could occur in two ways:
  - ✓ You reply to an email that asks for your personal or secretive information.
  - ✓ You open an attachment or a link provided in an email.
- The following is a list of information you should pay attention to before giving out:
  - ✓ ID number
  - ✓ Bank account number
  - ✓ Full Name Company you work for Credit card number
  - ✓ Credit limit
  - ✓ The number of cards you have Information about the last transaction you made.

**To report or inquire please call us any time at +974 4425 4040**

To report or inquire please call us:

**+974 4425 4040**

## Protect

- Update your computer and its programs on a regular basis.
- Update your browser and the browser's plug-ins regularly.
- Install the necessary software to protect your device, such as firewall, spam filters, anti-virus and anti-spyware, and ensure that they are updated regularly.
- Never type secretive (e.g. passwords or PIN) or personal information (e.g. name, location or salary) on shared or public devices.
- Check your transactions regularly. If you see any unusual transaction that you have not made contact Masraf Al Rayan immediately.
- Change your email or your online banking account passwords regularly.
- Do not include in your reply emails any personal information.

## Detect

- Avoid responding to an email that:
  - ✓ Contains jargons, poor grammar, or spelling mistakes.
  - ✓ Asks for your personal information.
  - ✓ Creates a sense of urgency.
  - ✓ Pretend to be from Masraf Al Rayan but not signed with the Masraf Al Rayan's logo or contact information.
- Never respond to calls or emails that ask for secret information such as: as PIN or passwords. Masraf Al Rayan will never ask for your PIN or password.
- Never respond to calls or emails that ask for personal or banking information e.g. credit card number, bank account number, id, name, or phone number.
- Verify the identity of your caller before giving out any of your personal information, and directly call Masraf Al Rayan's fraud line if there is any suspicion.
- Do not open email attachments unless you expect and trust them. It is also better to let your anti-virus program scan them first.
- Avoid opening URLs and attachments that you receive by email, unless you password resetting URLs).

## React

- Inform Masraf Al Rayan immediately about any suspicious email or phone call that asks for your banking information or personal information.
- Contact Masraf Al Rayan immediately if you believe that you have inadvertently given your personal or financial information while answering a phone call or an email.
- Change your email passwords and/or online banking account passwords immediately if you suspect that they may have been compromised.
- Contact Masraf Al Rayan immediately if you receive any transaction message that you do not recognize.

**To report or inquire please call us any time at +974 4425 4040**