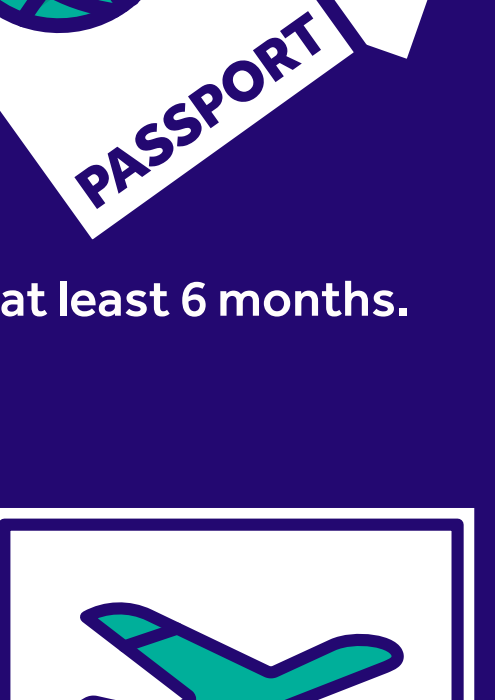
Safe financial Practices while abroad

بنك الرياض Riyad Bank | بكرة

Before Travel

DEPARTURE
PASSPORT
6+ MONTHS

- Make sure your passport is valid for at least 6 months.

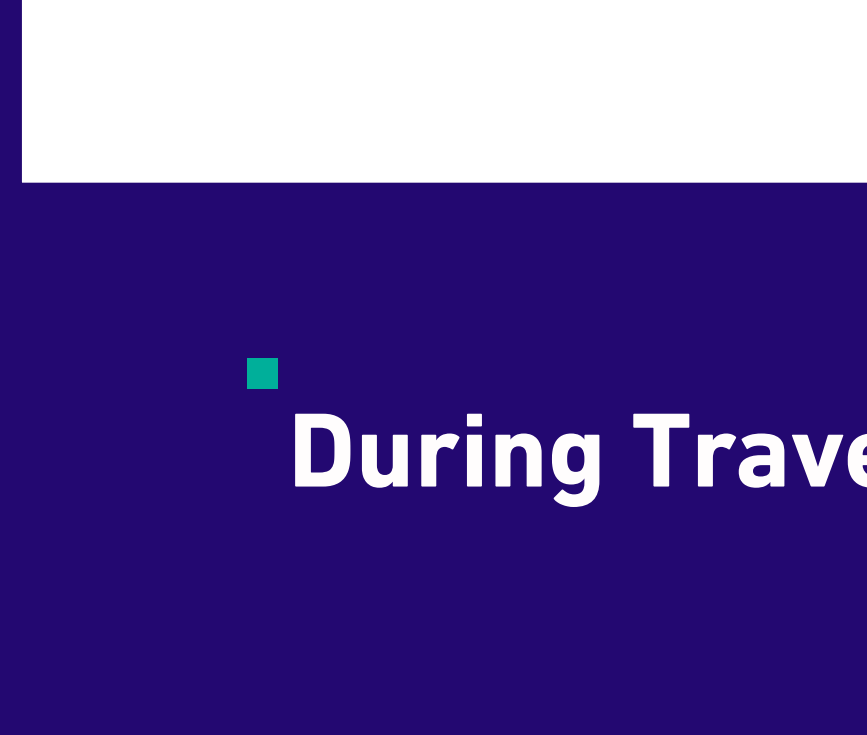


- Recognize the procedures for obtaining a visa by following up on what embassies post on their websites or through the local press.
- Ascertain the type of visa required (e.g., single or multiple) and the duration of its validity to enter and leave the countries to be visited.
- Fill in the application accurately with the required information when applying for the visa (whether it is for tourism, medical treatment, study, etc).

- Avoid traveling to troubled countries and regions with infectious diseases.

- ✓ Follow the rules and regulations issued by the security authorities of the countries you are visiting.
- ✓ Check your destination policy on carrying large cash amounts.
- ✓ You should deal solely with accredited local and international travel agencies that are officially licensed.
- ✓ Avoid keeping your bank details with airlines and hotels reservation sites.
- ✓ Make sure to activate the roaming service to follow up the bank notifications at the time of travel to track your financial transactions.
- ✓ Remember that relying solely on your phone for your reservations and using "Apple Pay" services for payment while traveling may expose you to many risks in the event of theft, God forbid.

During Traveling



- If you face any problem, call Saudi embassy in the country or contact any GCC mission.
- Register your passport in the country of arrival through the website of the Ministry of Foreign Affairs

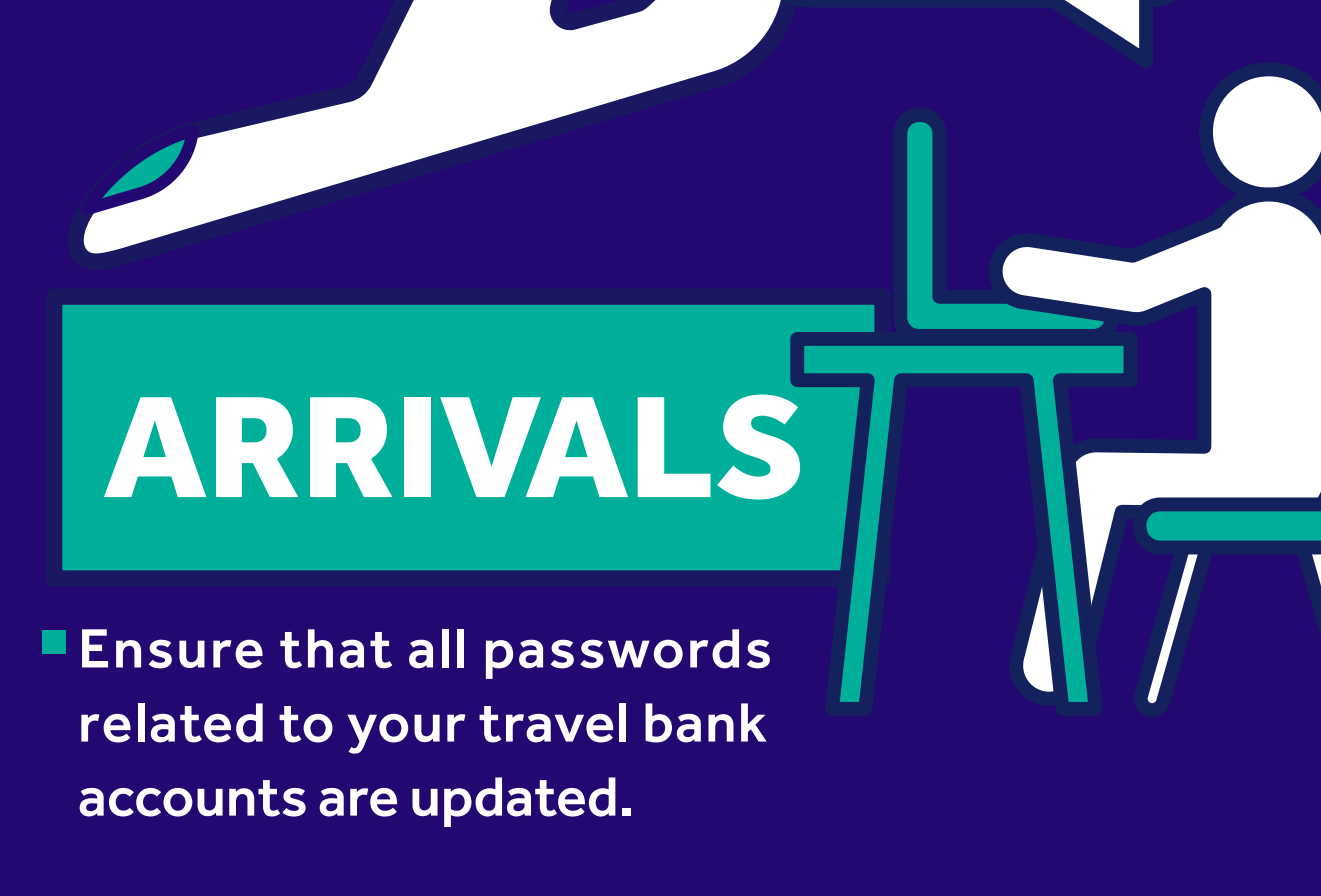
- Keep your valuables and copies of all travel and bank documents in a safe place.
- Keep your money, identification cards and bank cards in your front pockets or hand bag.
- Do not carry large amounts of cash while in public, and try to rely more on debit/credit cards.

- To avoid overcharges, always check your shopping receipts.
- It is better to use credit cards when shopping. Do not carry more cash than you need.
- Keep your bank card in a buffer wallet to avoid data erasure.
- Avoid speaking to strangers as they may attempt to distract you prior to theft.
- Only present your identification to official authorities when asked.
- Inform the closest police station when a theft occurs, along with the Saudi embassy, and the thief should not be tracked or clashed with.
- Do not allow credit card data to be photocopied or mortgage your identification cards at rental or housing offices.

- Always be aware of your personal belongings in crowded areas.
- Do not leave your card with the sales representative.
- Make sure to hide the triple digit behind the card.
- Guard yourself and don't talk to anyone when withdrawing money from a bank ATM machines.
- Be aware of different theft techniques such as collision and distraction schemes.
- Rent residence directly from well-known real estate offices and avoid signing unofficial residence contracts and carefully read the terms and conditions of the contracts.
- Do not excessively wear jewelry or carry anything that would draw attention.

- Rent residence directly from well-known real estate offices and avoid signing unofficial residence contracts and carefully read the terms and conditions of the contracts.

After travel



- Ensure that all passwords related to your travel bank accounts are updated.

Financial fraud

Avoid trusting random communications, financial fraud often occurs as a result of trusting fraudulent communications and messages from unreliable and dishonest people, and fraud occurs when sharing financial and account information with those people.

- **Cyber fraud** theft of confidential information: The fraudster usually sends an email to users or messages through mobile apps to obtain their personal information and account information, or redirects them to a website where they are required to enter personal information so that fraudsters can collect sensitive information such as user names, and passwords, and the details of the bank card by indicating that he is a trustworthy person or a well-known institution.
- **Embezzlement** possession of money or paper proving a right owned by another person with the intention of the owner
- **Financial scam** the use of deception to obtain an unlawful benefit.

Fraud style

SCAMMER
Please click here to activate the new security code.
Your card number **** will no longer be active.
Your shipment number is 99433212. Please pay the delivery fee through the following link.

- Impersonating a Government employee / Government agency.
- Impersonation of the service facilities sector.
- Hacking WhatsApp, a social networking account.
- Impersonate mail/shipping services.
- Impersonating relatives or friends.
- Impersonation of legal services / law firm.

- Impersonating a bank/bank employee.
- Impersonate another non-governmental company.
- Impersonating a charity/organization.
- Prizes and bonuses.
- Fake companies.

Procedures followed in the event of a fraud

- Direct contact with the bank to suspend accounts and cards through the bank's available channels.
- A report must be filed with the security authorities. 911
- Change passwords and user name instantly.

Phishing scammers use

- Usually, scammers use fake websites, e-mail imitating commercial brands, in order to steal personal information such as: names, numbers, passwords, security code, card digits and billing information

What does corporate email hacking mean?

- Criminals hack into email networks to obtain information about payment systems used by companies. They then deceive their employees into transferring money to their own bank accounts.

How can I tell if an email is fraudulent or not?

- Fraudulent emails typically ask you to provide personal information. Any email you receive from a trusted organization or entity such as banks, Amazon, or SAMACO, will not ask you for your password or other personal information. Regardless of what happens, do not share the verification code.

Messages to be cautious of when receiving them:

- Urgent requests for personal information.
- Warning phrases that ask you to take immediate action.
- Requests for (confidential) information, including
- Usernames, passwords and security codes.

How can you protect yourself from electronic fraud?

- **By keeping your personal information private and not sharing it with any untrusted parties. (Scammers' methods of accessing your data start with your response to them)**

Is there a penetration into the banking system?

Banks have strong and secure systems that block any attempts for fraud or scam, fraud attempts are usually made through targeting customers who share personal information and passwords.

What if you receive a call from the bank asking for your personal information?

Bank representatives do not have the right to ask for personal information or passwords over the phone, they only make the call to ask customers to go to the bank to update their information. If you receive such a call, do not share any personal information or passwords.

What should you DO if you Received a call or a text Requesting personal Information?

Report the incident to the number
330330

Stop the user name
Stop the account

Stop the ATM and credit cards

بنك الرياض Riyad Bank | بكرة