

Learn how to avoid Phishing and Vishing Scams

- In case of doubt, do not click on any link provided in the e-mail.
- Do not give any confidential information such as password, customer id, Credit/Debit Card number or PIN, CVV number, Date of Birth to any e-mail request.
- Do not open unexpected e-mail attachments or instant message download links.
- Always check the web address carefully before sharing any sensitive information.
- For logging in, always type the website address (www.bahrainisaudi.com) on your web browser.
- The Padlock icon at the upper or bottom right corner of the webpage must be always 'On' during secure transactions.
- Ensure that you have installed the latest anti-virus/ anti-spyware/ personal firewall/ security patches on your computer or high end mobile phones.
- Use non-admin user ID for daily work on your computer.
- Do not access Online Banking or make payments using your Credit/ Debit Card from shared or unprotected computers in public places.
- Do not call and leave any personal or account details on any telephone system, voice message, e-mail or an SMS
- Do not transfer funds to or share your account details with, unknown/ non-validated source, luring you with commission, attractive offers

Phishing Scam

If you receive any email or phone call requesting for your online banking details like PIN or password or credit / debit card number, please do not respond to it.

Vishing Scam

Contact your branch at a phone number you know to be accurate; appearing on the credit / debit card or Bank's statement or Bank's web site.

Please note that Bahraini Saudi Bank would not ask you to divulge any confidential information over email or phone.