

The client undertakes to refrain from the sending of any transfers for any illegal purpose such as, by way of example, sending transfers to usurious account or to the benefit of those promoting or managing gambling games or for the purchase of a prohibited commodity or other similar expenditures. The bank shall assume no responsibility whatsoever with respect to transfers that initiate or end up in violation of this clause.

KSA rules doesn't allow the remitter to remit money without knowing the beneficiary or without legal relation with the beneficiary or without legal purpose

Do not believe all ads on the Internet, especially those that offer goods at attractive prices that do not suit reality, so do not transfer any amount of money, even if it is a deposit or disclose your personal and bank data before making sure of the credibility of the advertisement

Fraudsters change their fraud methods quickly and periodically in order to get the largest number of victims, but below are common indicators of fraud:

- Unrealistic content or message (e.g., an email stating an unexpected credit or debit to your account)
- Rush to respond (scammers often use the language of urgency)
- Illogical and unrealistic returns on investments
- Very attractive and illogical prices, especially for goods or services
- Threatening language, such as stopping bank accounts if the caller does not respond
- Request to participate in personal banking, for example, security codes only for the customer, ATM card numbers"
- Unusual updating of beneficiary data.

Do not give the transaction reference number to anyone other than the person you intend to hand over the funds to.

"Q1": "Are the official government agencies (for example: the Saudi Central Bank, the Ministry of Commerce, Consumer Protection... etc) Requesting the transfer of money to deal with citizens' complaints?"

"A1": "Citizens are not required to transfer any amount in exchange for dealing or receiving citizens' complaints, and for more details, please check the official website of the governing authority or call directly on the numbers",

"Q2": "Are the official government agencies (for example: Saudi Central Bank, Ministry of Commerce, Consumer Protection, etc.) Require a money transfer for the purpose of upgrading your account for a refund?"

"A2": "The official authorities do not request a financial transfer to upgrade your account to a specific category to recover your money or process a refund. For more details, please check the official website of the governing authority or directly call the authorities main numbers.",

"Q3": "Are the official government agencies (for example: Saudi Central Bank, Ministry of Commerce, Consumer Protection, etc.) communicate using a mobile number or using an unofficial number?"

"A3": "Official government agencies never communicate through mobile numbers or unofficial numbers.",

"Q4": "Are the official government agencies (for example: Saudi Central Bank, Ministry of Commerce, Consumer Protection, etc.) communicate with citizens via WhatsApp?"

"A4": "Official government agencies do not communicate over WhatsApp from mobile numbers or unofficial numbers.",

"Q5": "Do the official government agencies (for example: Saudi Central Bank, Ministry of Commerce, Consumer Protection, etc.) require sharing the bank's one-time security code?"

"A5": "We emphasize that these security codes are only for you to complete your financial operations and are not shareable with others. The official government agencies will never request the one-time security code intended to complete financial operations on your personal account.",

"Q6": "Is it required to share the ATM card number over the phone to update the account details at the bank?"

"A6": "The bank does not update the account data by contacting you, and does not require sharing the ATM card number to update the account data, and you can update your account data through the Al Rajhi application or by visiting one of the bank branches.",

"Q7": "How can I identify the official investment authorities?"

"A7": "The investment is not done by individuals and done by official parties and can be identified by visiting the Capital Market Authority website, or by conducting a simple search for the company",

"Q8": "Are all advertisements on the Internet reliable and secure to deal even with the emergence of security protocols (HTTPS)?"

"A8": "Not all ads on the Internet are safe, do not believe all ads on the Internet, especially those that offer goods at attractive prices that do not suit reality, so do not transfer any amount of money, even if it is a deposit or disclose your personal and bank data before making sure of the credibility of the advertisement.",

"Q9": "What are the indicators of cyber fraud and how can I identify the ways?"

"A9": "Fraudsters change their fraud methods quickly and periodically in order to get the largest number of victims, but below are common indicators of fraud:\n• Unrealistic content or message (e.g., an email stating an unexpected credit or debit to your account)\n• Rush to respond (scammers often use the language of urgency)\n• Illogical and unrealistic returns on investments\n• Very attractive and illogical prices, especially for goods or services\n• Threatening language, such as stopping bank accounts if the caller does not respond\n• Request to participate in personal banking, for example, security codes only for the customer, ATM card numbers"

لا يجوز للعضو أن يستغل عضويته لإرسال حوالات لأي غرض محرم شرعا كإرسالها على سبيل المثال لا الحصر بغرض إضافتها لحسابات روية أو لصالح من يروج لألعاب الميسر أو من يديرها أو بغرض شراء سلعة محرمة شرعا أو غير ذلك من أوجه مشابهة و لا يتحمل المصرف أي مسئولية بشأن أي حوالات من هذا النوع. استهلالا أو مالا.

أنظمة المملكة تمنع تحويل أموال دون معرفة العميل المحول بالمستفيد (المحول إليه) أو دون علاقة نظامية تربطه بالمستفيد أو دون غرض مشروع

لا تصدق جميع الاعلانات في الانترنت وخاصة التي تقوم بعرض سلع بأسعار مغرية لا تتناسب مع الواقع ، لذلك لا تقم بتحويل اي مبلغ مالي حتى ولو كان عربون او الاقصاد عن بياناتك الشخصية والبنكية قبل التأكد من مصداقية الاعلان ،

المحتالون يغيرون طرق احتيالهم بشكل سريع و ودوري وذلك للحصول على اكبر قدر من الضحايا ، ولكن يوجد مؤشرات تدل على الاحتيال مثل :

- محتوى او رسالة غير واقعية (على سبيل المثال : بريد الكتروني يفيد بخصم من حسابك غير متوقع)
- الاستعجال بالرد (المحتالون غالبا ما يستخدمون لغة الاستعجال)
- العوائد الغير منطقية بالاستثمار
- الاسعار المغرية جدا والغير منطقية وخاصة للسلع.
- لغة التهديد كإيقاف الحسابات المصرفية في حال عدم التجاوب للمتصل
- طلب مشاركة بيانات شخصية بنكية مثلا رموز امان خاصة فقط بالعميل ، ارقام بطاقة الصراف الالي
- تحديث بيانات المستفيد بشكل غير اعتيادي

لا تعطي رقم مرجع المعاملة لأي شخص آخر غير الشخص الذي تنوي تسليم الأموال له

"Q1": "هل الجهات الرسمية الحكومية (على سبيل المثال : البنك المركزي السعودي ، وزارة التجارة ، حماية المستهلك... الخ) تطلب تحويل مبلغ مالي للتعامل مع شكاوي المواطنين؟"

"A1": "لا يطلب من المواطنين تحويل اي مبلغ مالي مقابل التعامل او تلقي شكاوي المواطنين ، ولتفاصيل اكثر يرجى مراجعة الموقع الرسمي للجهة الحكومية أو الاتصال المباشر على الارقام الرسمية"

"Q2": "هل الجهات الرسمية الحكومية (على سبيل المثال : البنك المركزي السعودي ، وزارة التجارة ، حماية المستهلك ... الخ) تطلب تحويل اموال بغرض ترقية حسابك لاسترداد الاموال؟"

"A2": "لا تقوم الجهات الرسمية بطلب تحويل مالي لترقية حسابك الى فئة معينة لاسترداد اموالك من الجهات الرسمية ولتفاصيل اكثر يرجى مراجعة الموقع الرسمي للجهة الحكومية أو الاتصال المباشر على الارقام الرسمية"

"Q3": "هل الجهات الرسمية الحكومية (على سبيل المثال : البنك المركزي السعودي ، وزارة التجارة ، حماية المستهلك ... الخ) تقوم بالتواصل من رقم جوال او رقم غير رسمي؟"

"A3": "لا تقوم الجهات الرسمية الحكومية بالتواصل من خلال ارقام جولات او ارقام غير رسمية"

"Q4": "هل الجهات الرسمية الحكومية (على سبيل المثال : البنك المركزي السعودي ، وزارة التجارة ، حماية المستهلك ... الخ) تقوم بالتواصل مع المواطنين عن طريق الواتس اب؟"

"A4": "لا تقوم الجهات الرسمية الحكومية بالتواصل عن طريق الواتس اب من ارقام جولات او ارقام غير رسمية"

"Q5": "هل الجهات الرسمية الحكومية (على سبيل المثال : البنك المركزي السعودي ، وزارة التجارة ، حماية المستهلك ... الخ) تطلب مشاركة رمز الامان لمره واحده الخاص بالمصرف؟"

"A5": "نؤكد على انه هذه الرموز الامان خاصة فقط بك لاتمام عملياتك المالية و غير قابلة للمشاركة مع الاخرين ، كما انه الجهات الرسمية الحكومية لا تقوم بطلب رمز الامان لمره واحده والمخصص لاتمام عمليات مالية على حسابك الشخصي"

"Q6": "هل يتطلب مشاركة رقم بطاقة الصراف الالي عبر الهاتف لتحديث بيانات الحساب بالمصرف؟"

"A6": "لا يقوم المصرف بتحديث بيانات الحساب عن طريق الاتصال بك ، و لا يتطلب مشاركة رقم بطاقة الصراف الالي لتحديث بيانات الحساب ، ويمكنك تحديث بياناتك حسابك من خلال تطبيق الراجحي او زيارة احد الفروع"

"Q7": "كيف يمكنني التعرف على الجهات الرسمية للاستثمار؟"

"A7": "الاستثمار لا يتم عن طريق افراد ويتم فقط عن طريق جهات رسمية ويمكن التعرف عليها زيارة موقع هيئة سوق المال ، او باجراء بحث بسيط عن الشركة"

"Q8": "هل جميع الاعلانات في شبكة الانترنت مؤتوقة وامنة للتعامل حتى مع ظهور بروتوكولات الامان (HTTPS)؟"

"A8": "ليست جميع الاعلانات في شبكة الانترنت امنة ، لا تصدق جميع الاعلانات في الانترنت وخاصة التي تقوم بعرض سلع بأسعار مغرية لا تتناسب مع الواقع ، لذلك لا تقم بتحويل اي مبلغ مالي حتى ولو كان عربون او الاقصاد عن بياناتك الشخصية والبنكية قبل التأكد من مصداقية الاعلان"

"Q9": "ماهي مؤشرات الاحتيال السيبراني وكيف يمكنني التعرف على طرق المحتالين؟"

"A9": "المحتالون يغيرون طرق احتيالهم بشكل سريع و ودوري وذلك للحصول على اكبر قدر من الضحايا ، ولكن يوجد مؤشرات تدل على الاحتيال:\n• محتوى او رسالة غير واقعية (على سبيل المثال : بريد الكتروني يفيد بخصم من حسابك غير متوقع)\n• الاستعجال بالرد (المحتالون غالبا ما يستخدمون لغة الاستعجال)\n• العوائد الغير منطقية بالاستثمار\n• الاسعار المغرية جدا والغير منطقية وخاصة للسلع\n• لغة التهديد كإيقاف الحسابات المصرفية في حال عدم التجاوب للمتصل\n• طلب مشاركة بيانات شخصية بنكية مثلا رموز امان خاصة فقط بالعميل ، ارقام بطاقة الصراف الالي"