بـــوبـــيـــان
Boubyan

نصائح للحماية من الاحتيال

Fraud Protection Security Tips

لنكن على دراية

الحملة التوعوية المصرفية

EN ع

يوليو، 2025

July, 2025

في وقتنا الحالي، طرق الاحتيال صارت كثيرة ومتنوعة، والمحتالين يستخدمون كل الوسائل عشان يوصلون لمعلوماتك البنكية. عشان جذي، لازم نكون واعين.

نقدم لك بعض النصائح المهمة لحماية نفسك وبياناتك الشخصية من الاحتيال

نصائح عامة:

🔒 لا تضغط على الروابط المشبوهة

إذا وصلك رابط من رقم أو إيميل مو معروف، لا تفتحه

🔐 خلك حريص على حساباتك

استخدم باسوورد قوي غير عن باقي الحسابات، وفعّل خاصية التحقق بخطوتين، ولا تفتح أي ملف أو رابط ما طلبته

📱 لا تنشر معلوماتك الخاصة على مواقع التواصل

لأن هالشي يساعد المحتالين في اختراق حساباتك أو ممكن يستخدمونها عشان يخمنون شنو كلمة السر أو أسئلة الأمان

🛡️ إذا شكّيت، تأكد

اسأل شخص تثق فيه أو زور الموقع الرسمي قبل اتخاذ أي إجراء من أي رسالة مو متأكد من مصدرها أو مشبوهة

نصائح أثناء السفر!

🏧 أجهزة السحب الآلي المشبوهة

- اسحب من أجهزة السحب اللي داخل البنوك أو المجمعات، وابتعد عن اللي بالشارع
- إذا علقت بطاقتك في جهاز السحب الآلي، وقّف البطاقة على طول من خلال التطبيق

📲 الاحتيال عبر نقاط البيع

خل بطاقتك معاك دايماً، ويفضل تستخدم الدفع بدون لمس أو من خلال المحفظة الإلكترونية

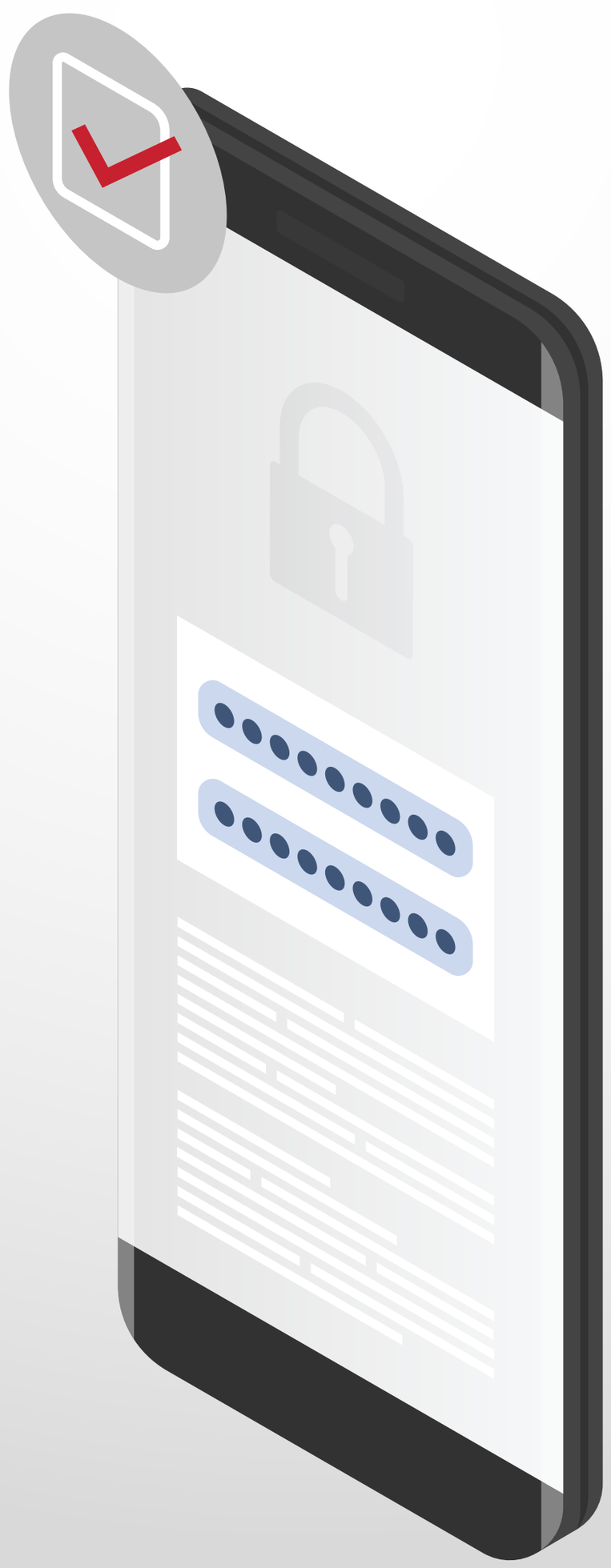
نصائح أثناء السفر!

⚠️ احذر من العروض الوهمية

- تأكد من موقع الفندق وعنوانه عبر الإنترنت
- احجز من مواقع حجوزات سفر معروفة
- لا تحول أي مبلغ حق شخص ماتعرفه
- تأكد من الحساب قبل لا تدفع، واستخدم طرق دفع آمنة
- العرض اللي يكون وايد قوي غالباً يكون غير حقيقي

🚨الاحتيال عبر رموز الـ QR

في ناس يحطون رموز QR مزيفة بمواقف السيارات أو محطات البانزين. قبل لا تدفع، تأكد من المصدر والرابط عدل



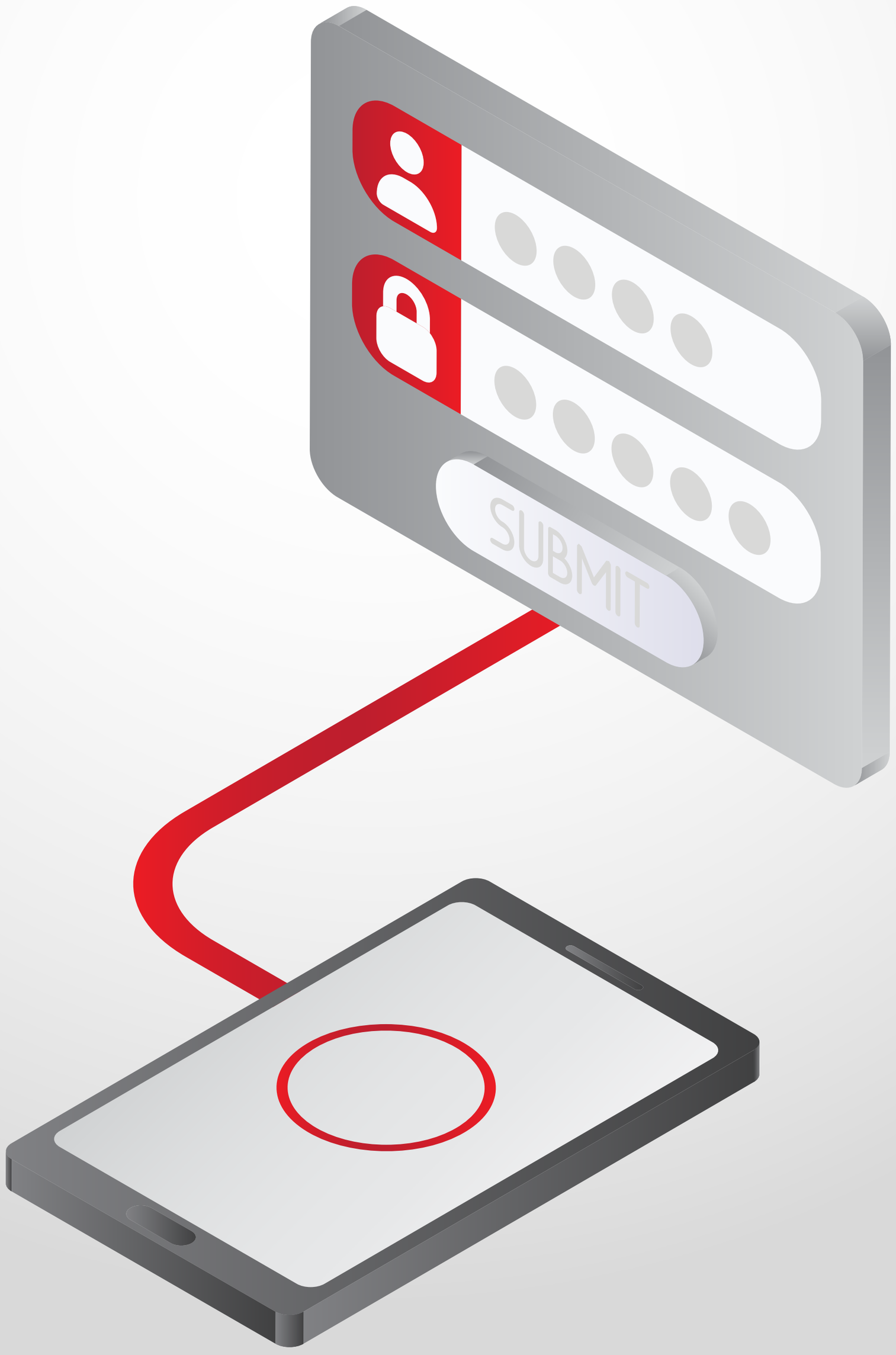
طرق أخرى للاحتيال:

📞 احذر من الاحتيال عبر المكالمات الهاتفية

- ممكن يكلمك أحد ويقول إنه من البنك أو جهة حكومية، ويحذرك بهدف أنه يخوفك عشان تعطيه معلوماتك
- لا تشارك بياناتك المصرفية أو رموز OTP
- إذ شكّيت يفضل انك تنهي المكالمة وتتصل برقم رسمي للتأكد من الجهة

🔑 لا تشارك رمز الـOTP مع أي شخص

- لا تعطي رمز التحقق لأي أحد، خصوصاً اللي يتصل فيك فجأة
- لا تحمّل تطبيقات تحكم بجهازك عن بعد إلا إذا كنت متأكد



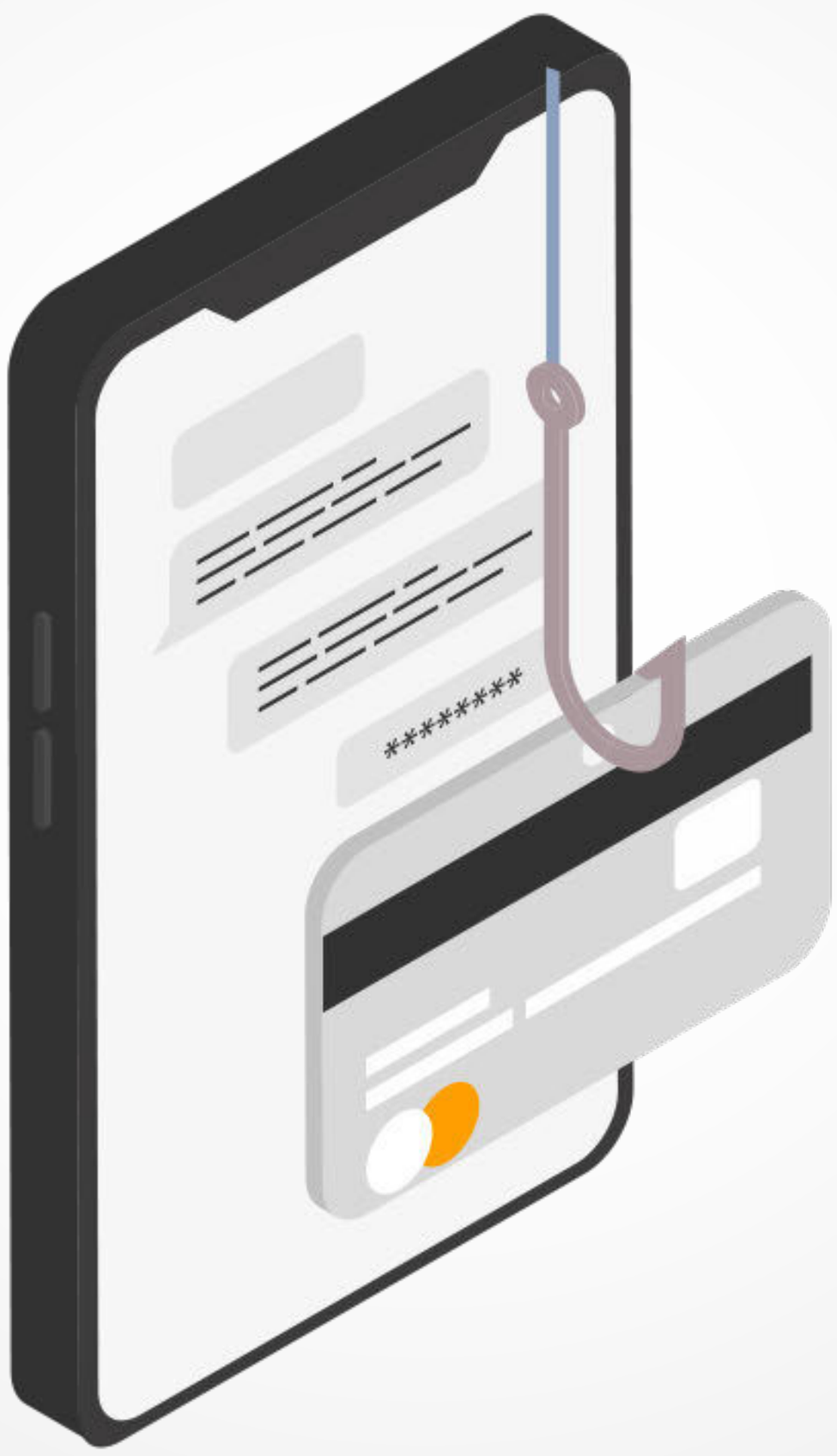
التسوق عبر الإنترنت:

🌐 تأكد من الموقع

الموقع لازم يبدأ بـ https:// وما يكون فيه أخطاء إملائية أو حروف غريبة بالرابط

💸 انتبه من طرق الدفع المشبوهة

طرق الاحتيال الشائعة: الدفع من خلال التحويل أو بطاقات الهدايا أو عملات رقمية أو كاش



إذا شكيت بعملية احتيال، قم بإيقاف البطاقة مؤقتاً من خلال التطبيق وتواصل مع مركز الاتصال الخاص ببنك بوبيان على 1820082 داخل الكويت أو 22282000 965+ من خارج الكويت

بنك بوبيان دايماً معاك

Fraudsters are getting smarter and sneakier!
That's why it's important to stay alert and protect yourself when it comes to your personal and banking information.

Here are a few friendly reminders to help you stay secure.

Generic Cybersecurity Tips:

🔒 Avoid clicking on suspicious links

Do not click on links in emails or text messages from unknown or untrusted sources

🔐 Follow cybersecurity best practices

Use strong, unique passwords for each account, enable multi-factor authentication, and avoid downloading or opening unsolicited attachment or links

📱 Be cautious on social media

Avoid posting personal information that could help scammers guess your passwords or answer your security questions

🛡️ If unsure, stop and verify

Talk to someone you trust or visit the official website of the company before acting on any suspicious message

Travel Smart, Stay Secure!

🏧 ATM Skimming

- Use secure ATMs for cash withdrawals located in Banks or malls
- If your card gets stuck in the ATM, immediately stop your card through the Mobile App to prevent unauthorized use

📲 POS Scam

Keep your card in sight and instead use contactless or mobile wallet payments for added security

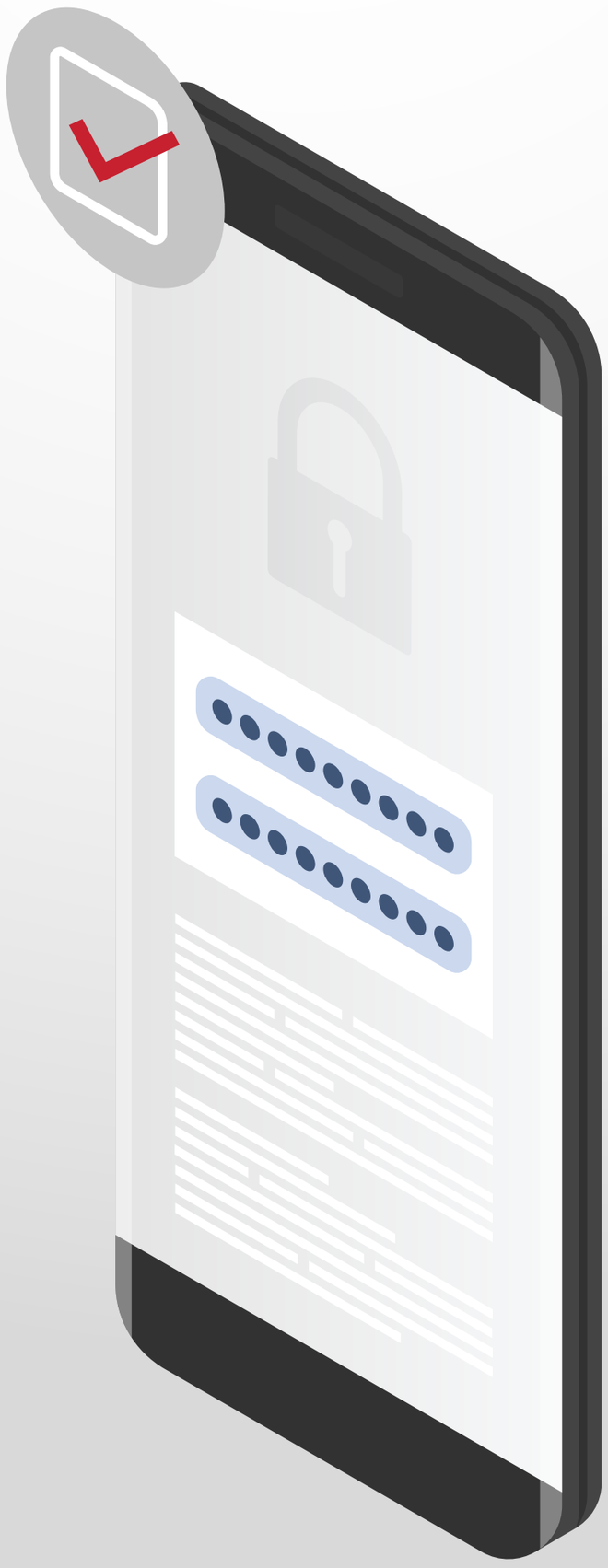
Travel Smart, Stay Secure!

⚠️Be cautious from Fake Offerings

- Search the address online to verify it's a real accommodation
- Use only trusted travel booking platforms or known travel websites
- Never send cash or wire transfers to individuals
- Make sure the business has a verified account and use secure payment channels
- If the deal sounds too good to be true, it is probably fake

🚨QR Code Phishing Alert

- Scammers may place fake QR codes (for example at car parking meters or electric car charging meters) that redirect you to look-alike payment sites to steal your info.
- Always check that the QR code is from a trusted source and review the URL carefully before paying.



Other Types of Fraud:

📞 Beware of Phone Scams (Phishing)

- Scammers may call pretending to be from your bank, tech support, or a government agency. They often create a sense of urgency to pressure you into revealing personal or financial information.
- Do not share account details, PINs, or one-time passcodes over the phone.
- Hang up and call back using a verified number if you're unsure

🔑 Never share your one-time passcode (OTP)

- Do not share your passcode with anyone, especially unsolicited callers or messages.
- Never install remote access software unless you are certain it's from a trusted source.

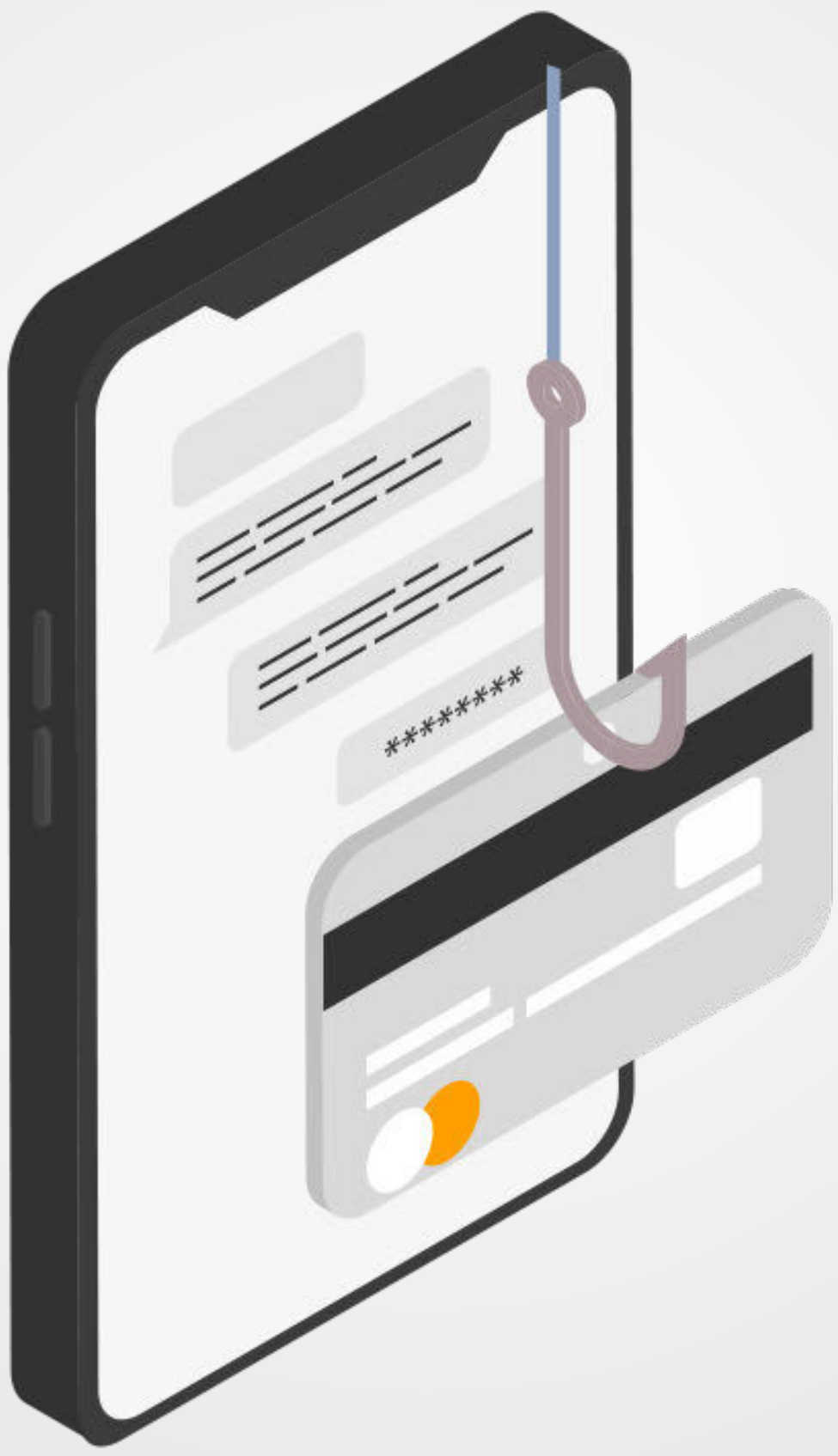
Online Activity / e-Commerce:

🌐 Look for secure websites

When shopping or banking online, check that the website starts with “https://” and the page name doesn’t contain spelling errors or strange characters

💸 Watch out for scam payment requests

Be cautious if someone asks you to pay via wire transfers, prepaid gift cards, cryptocurrency, or cash—these are common signs of fraud.



If you suspect fraud, please pause your card via the mobile app and contact Boubyan call center immediately on 1820082 from inside Kuwait
and +965 22282000 from outside Kuwait

Stay safe,
Boubyan Bank