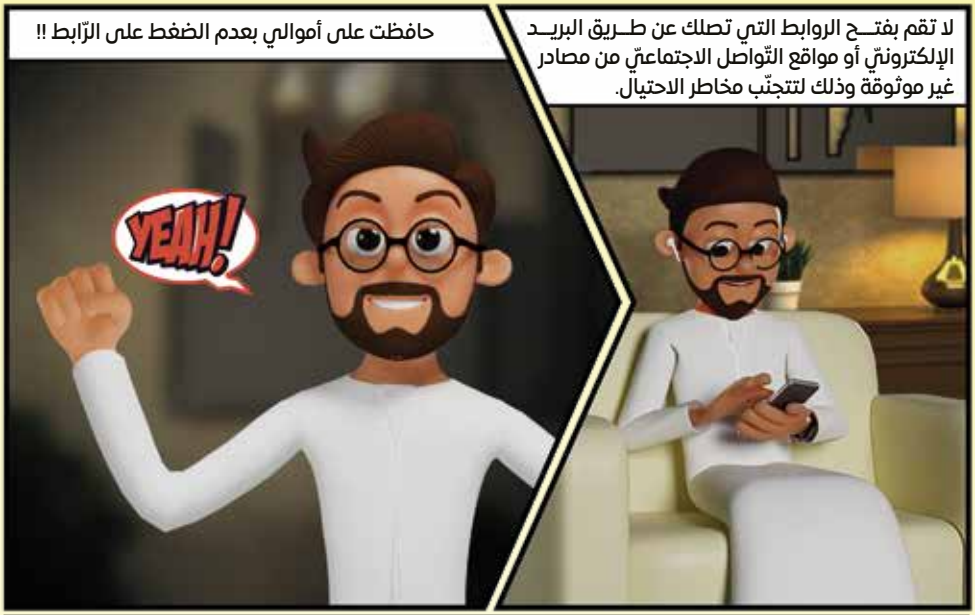
سلسلة آدم
للوقاية من الاحتيال

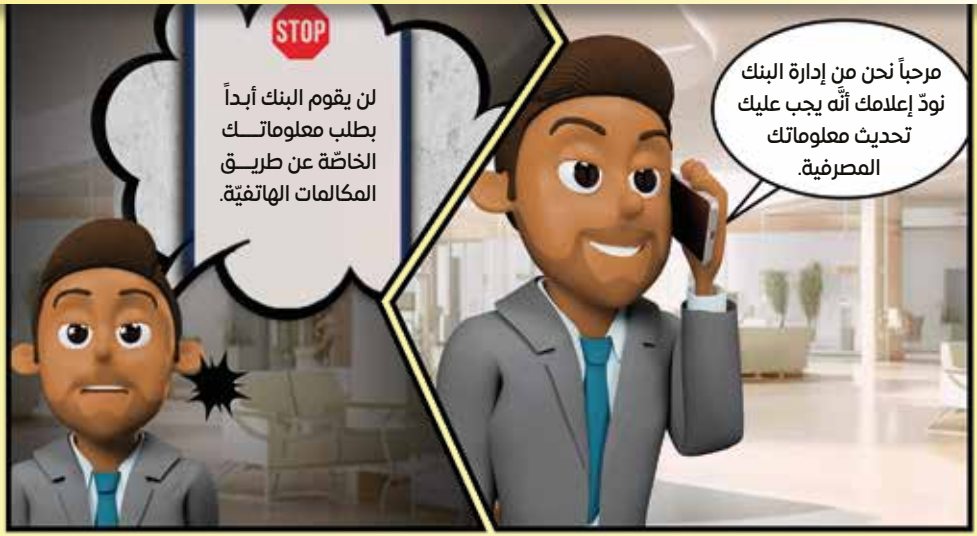
تم إعداد هذا الكتيّب لمساعدتك في التعرُّف على أنشطة الاحتيال المحتملة وكيفية مواجهتها. ننصحك بشدّة بتصفّح هذا الكتيّب بتمعّن لتكون على دراية بالإجراءات الاستباقيّة الموضّحة لتحمي نفسك من الوقوع ضحيّةً للاحتيال.

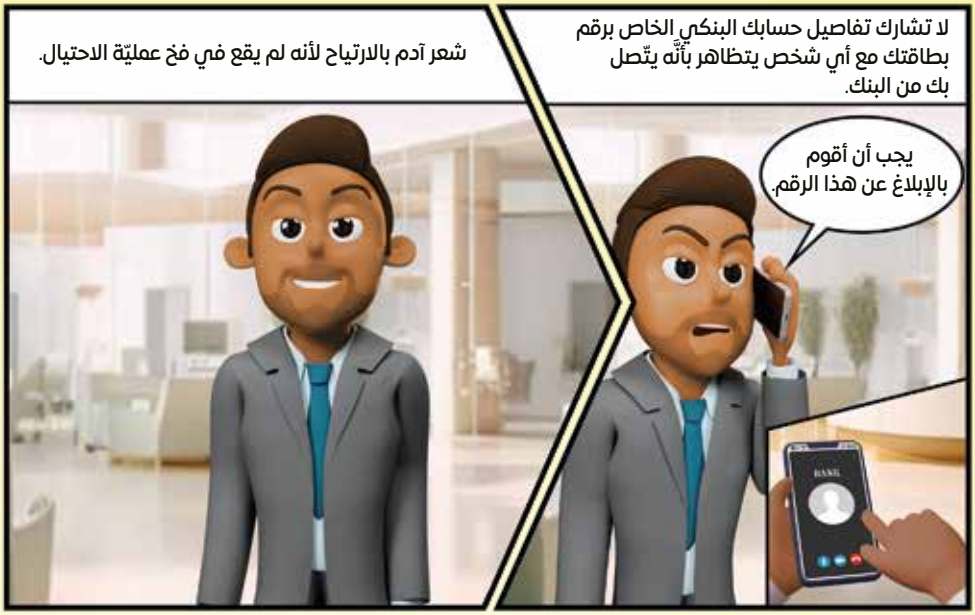
التصيّد الاحتياليّ عبر الانترنت



- تجنّب الصّفقات والعروض المغرية الّتي تكاد لا تصدق.
- لا تضغط على الرّوابط الواردة عبر رسائل البريد الإلكترونيّ/الرسائل النصية /وسائل التّواصل الاجتماعيّ من مصادر غير موثوقة.
- قم دائماً بالتحقّق من العروض من خلال القنوات الرسميّة للمتاجر.

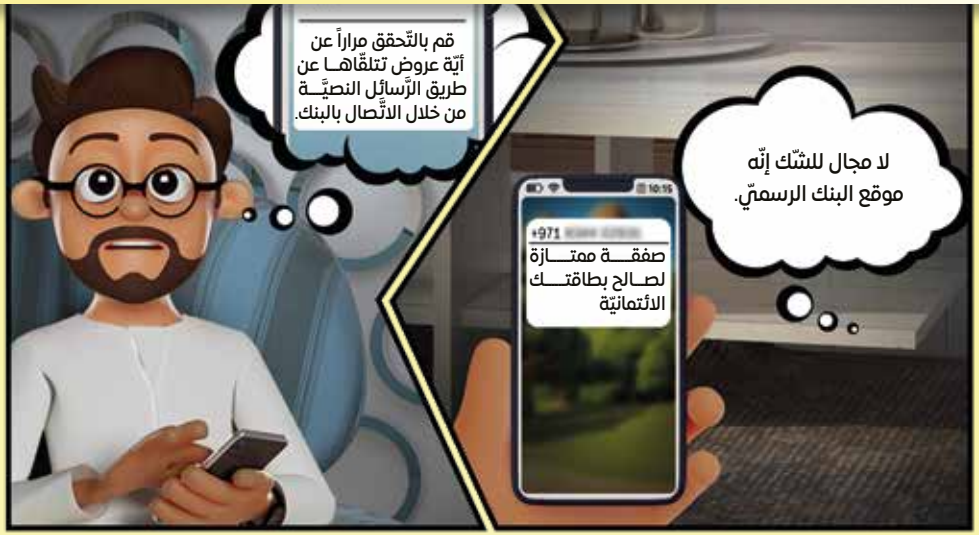
التصيّد الاحتياليّ عبر المكالمات الصوتيّة

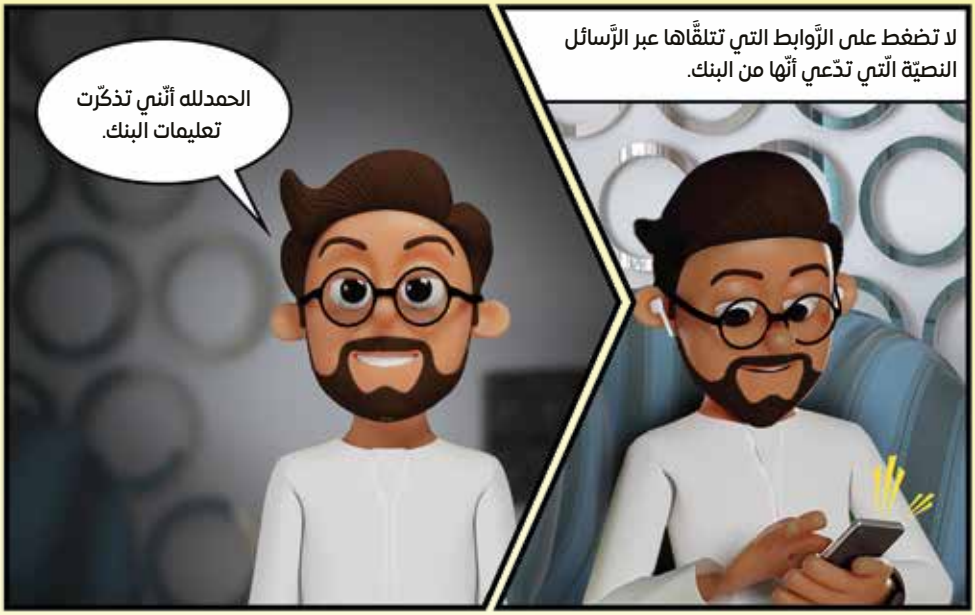




- لا تشارك (رقم البطاقة أو تاريخ انتهاء الصلاحيّة أو رقم CVV) أو تفاصيل حسابك المصرفيّ (اسم الحساب ورقم الحساب) مع أي شخص يتظاهر بأنَّه يتّصل بك من البنك/السّلطات/الشّرطة.
- قم بالإبلاغ عن مثل هذه المكالمات إلى الشّرطة/ البنك الّذي تتعامل معه.
- لن تطلب البنوك أو السّلطات أبداً معلوماتك الخاصّة أثناء المكالمات الهاتفيّة.

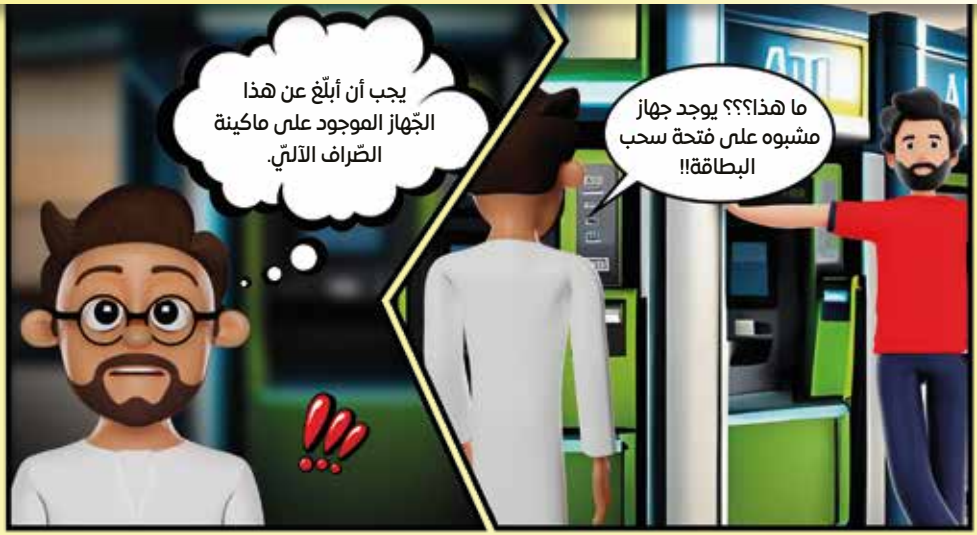
التصيّد الاحتياليّ عبر الرّسائل النصيّة

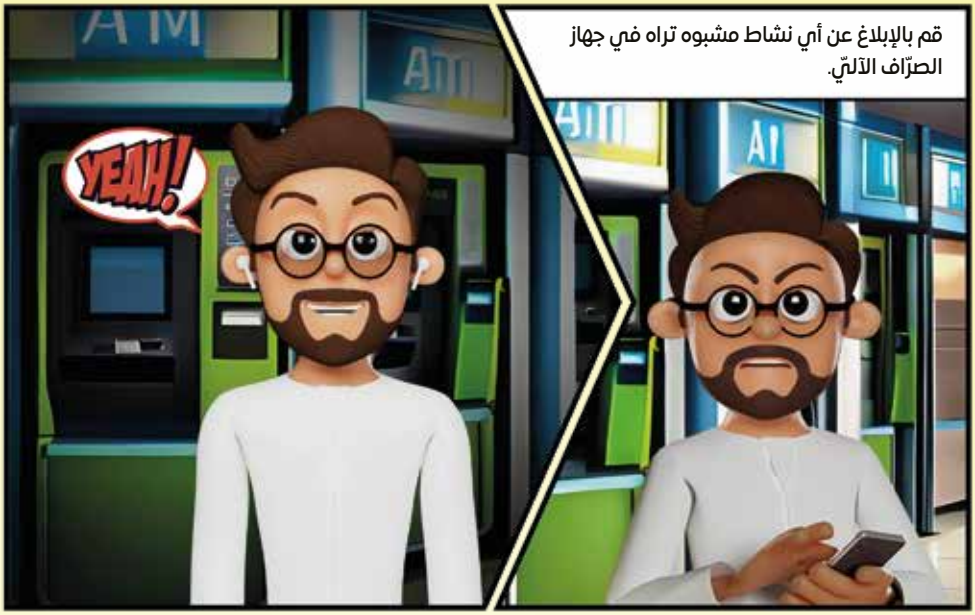




- كن حذراً عند الضغط على أيّ رابط تتلقّاه خاصّة عندما يتعلق الأمر بمعاملات ماليّة أو تفاصيل شخصيّة.
- قم بالإبلاغ عن حالات الاحتيال إلى السّلطات والتحقّق من العروض مباشرةً مع البنك.
- تحقّق دائماً من مصدر هذه الرسائل.

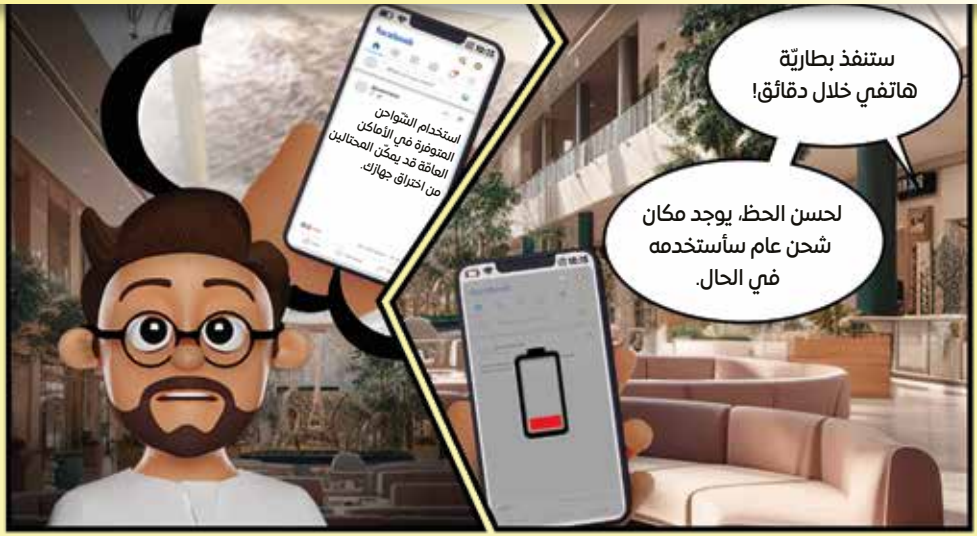
نسخ بطاقة الصرّاف الآليّ

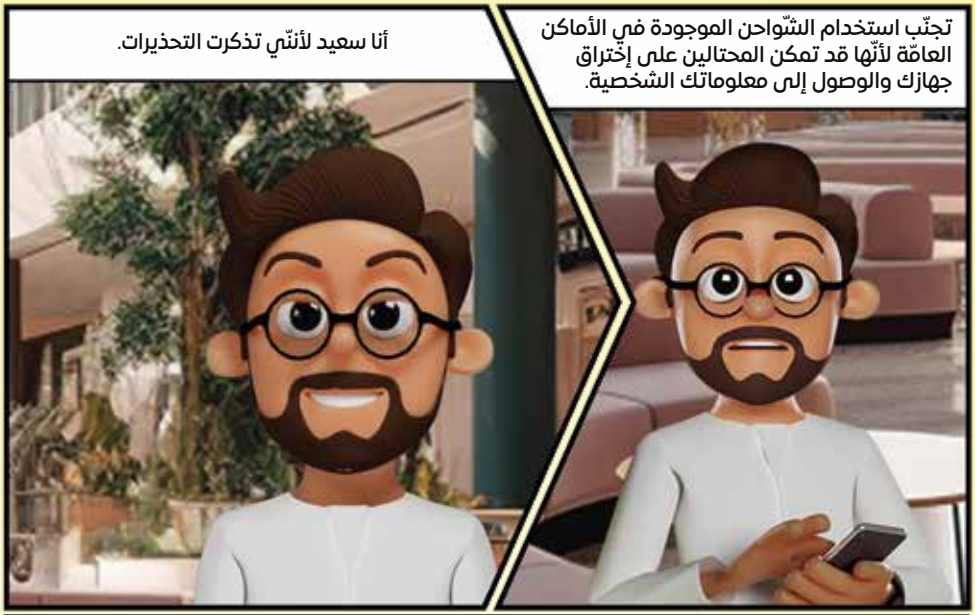




- كن يقظاً دائماً أثناء استخدام أجهزة الصرّاف الآليّ وأبلغ عن أي أنشطة مشبوهة.
- لا تقبل أبداً المساعدة من الغرباء عند أجهزة الصرّاف الآليّ.
- اتصل بالبنك حالاً في حال علقت البطاقة في الجهاز.
- تأكد أن لا أحد يحاول رصد الرمز السري للبطاقة.

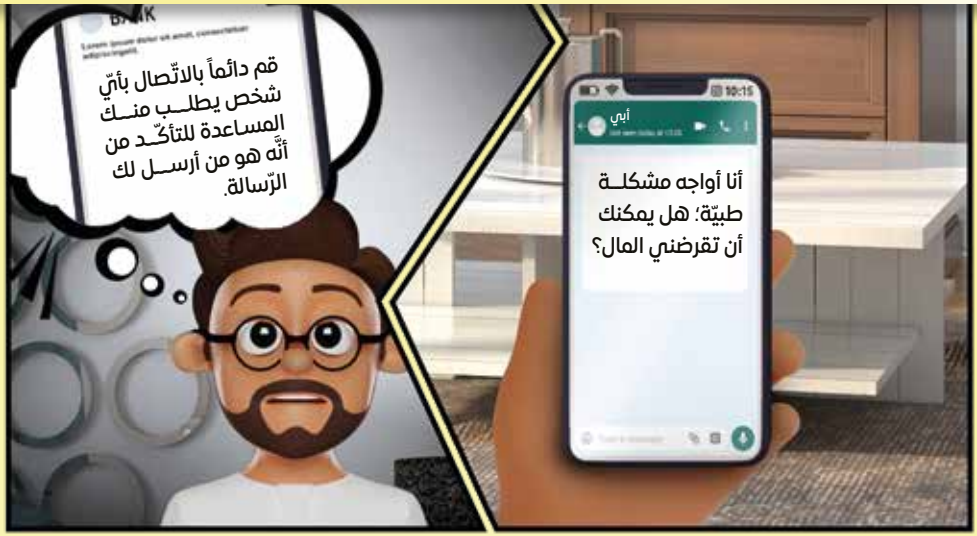
الاحتيال عن طريق منافذ الشحن العمومية





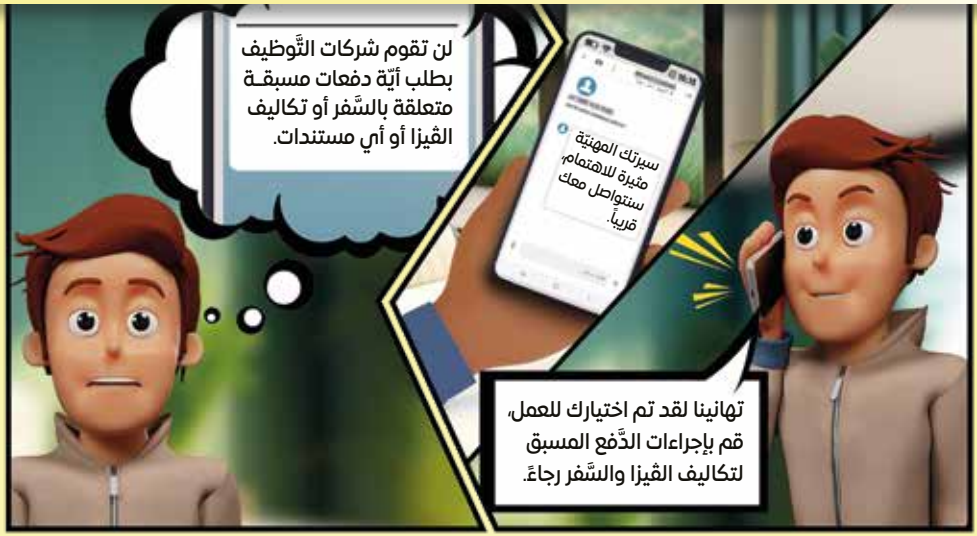
- تجنب محطّات الشّحن العامّة واستخدم وصلات الUSB الخاصّة بك لاستخدامها في المنافذ الإلكترونيّة.
- قم بالاحتفاظ بشاحن محمول معك للشّحن في أي مكان دون اللجوء لاستخدام الشواحن العامّة.

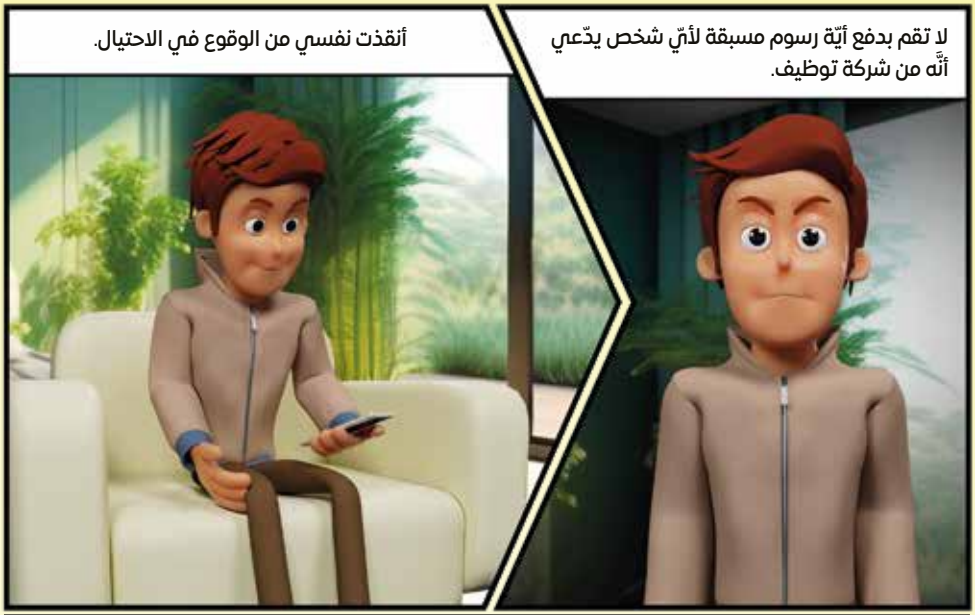
انتحال الهويّة عبر مواقع التّواصل الاجتماعيّ



- امتنع عن مشاركة تفاصيل بطاقة ائتمانك عبر مواقع التّواصل الاجتماعيّ، والبريد الإلكترونيّ، وتطبيقات الرّسائل.
- تذكَّر أهميّة التأكّد من صحّة الطّلبات المستعجلة الّتي تصل عبر مواقع التّواصل الاجتماعيّ أو البريد الإلكترونيّ أو المكالمات الهاتفيّة.
- قم بالإتصال هاتفياً للتأكد من صحة الرسائل المرسلة.

احتيال الوظائف عبر الإنترنت



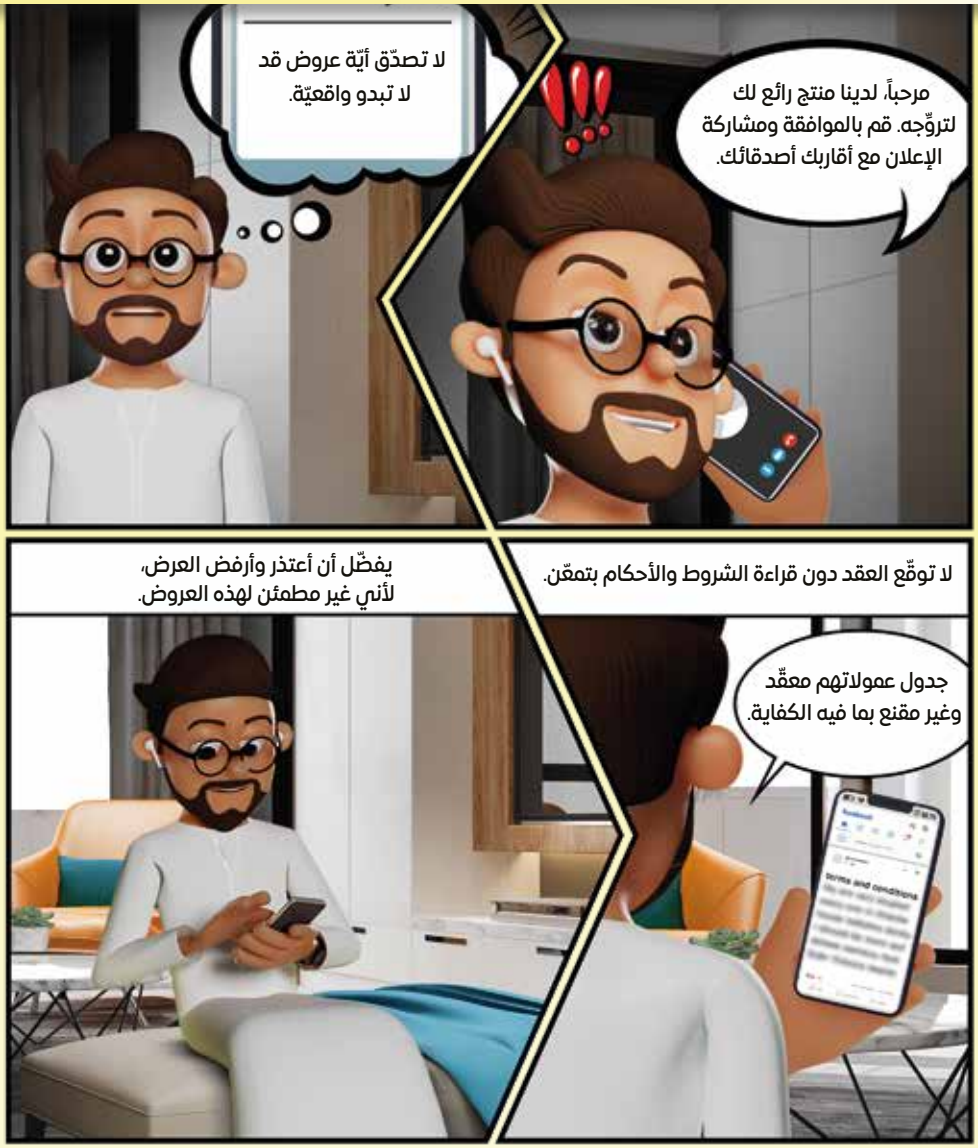


- فرص العمل التي على الإنترنت قد تكون محاولات إحتيالية.
- على الباحثين عن العمل توخّي الحذر فيما يتعلَّق بالدّفع المسبق أو إعطاء معلومات ماليّة كجزء من استمارة التّقديم على العمل.
- يُعد التأكّد من صحّة فرص العمل أمر أساسيّ عبر البحث عن حسابات العمل الرسميّة أو التواصل المباشر.

اتحاد مصارف الإمارات

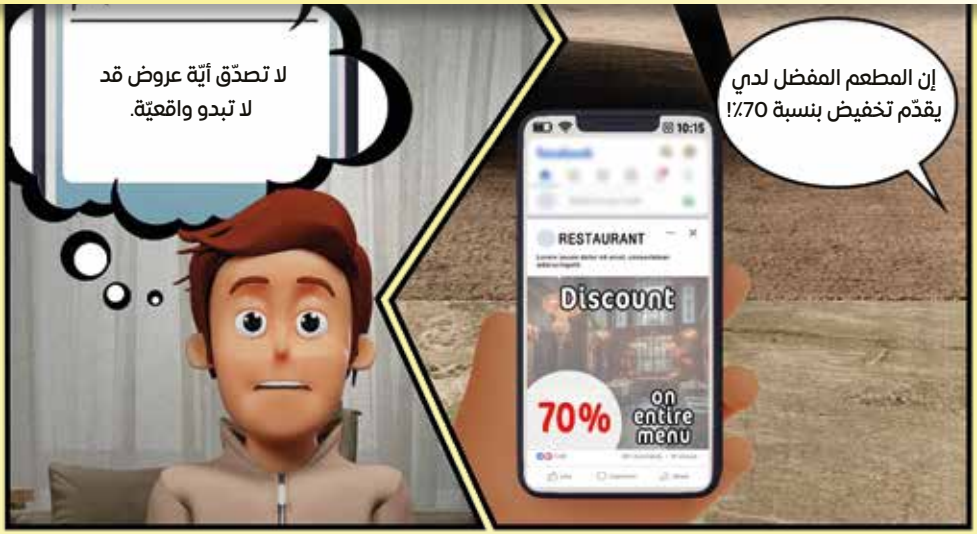
UAE BANKS FEDERATION

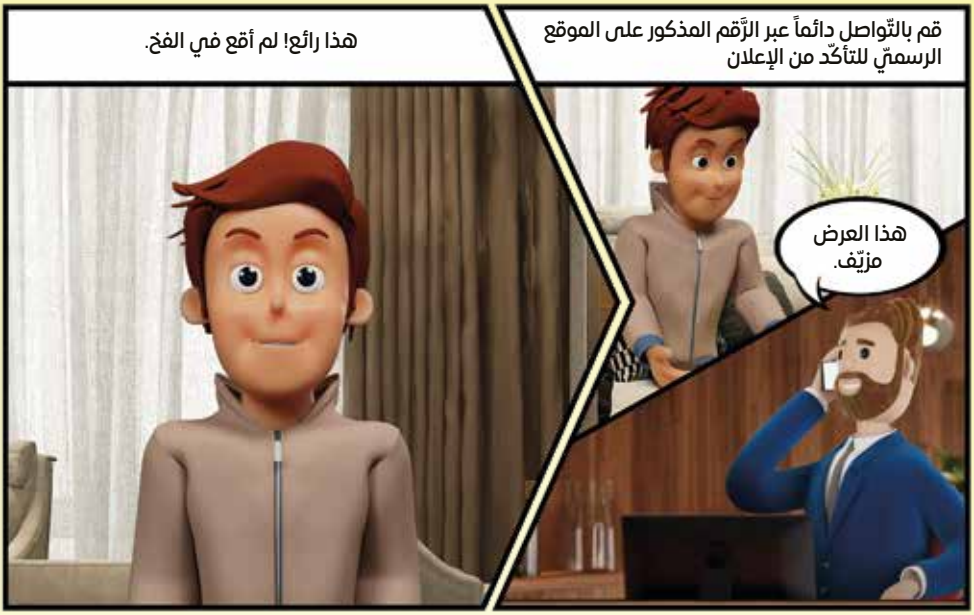
الاحتيال الهرميّ التسويقيّ



- ابقَ حذرعندما يُقدَّم لك عروض تبدو رائعة.
- مراجعة وفهم العقود يحميك من التعرّض للاحتيال.
- توخَّ الحذر دائماً عند التفكير بالموافقة على أي عرض.

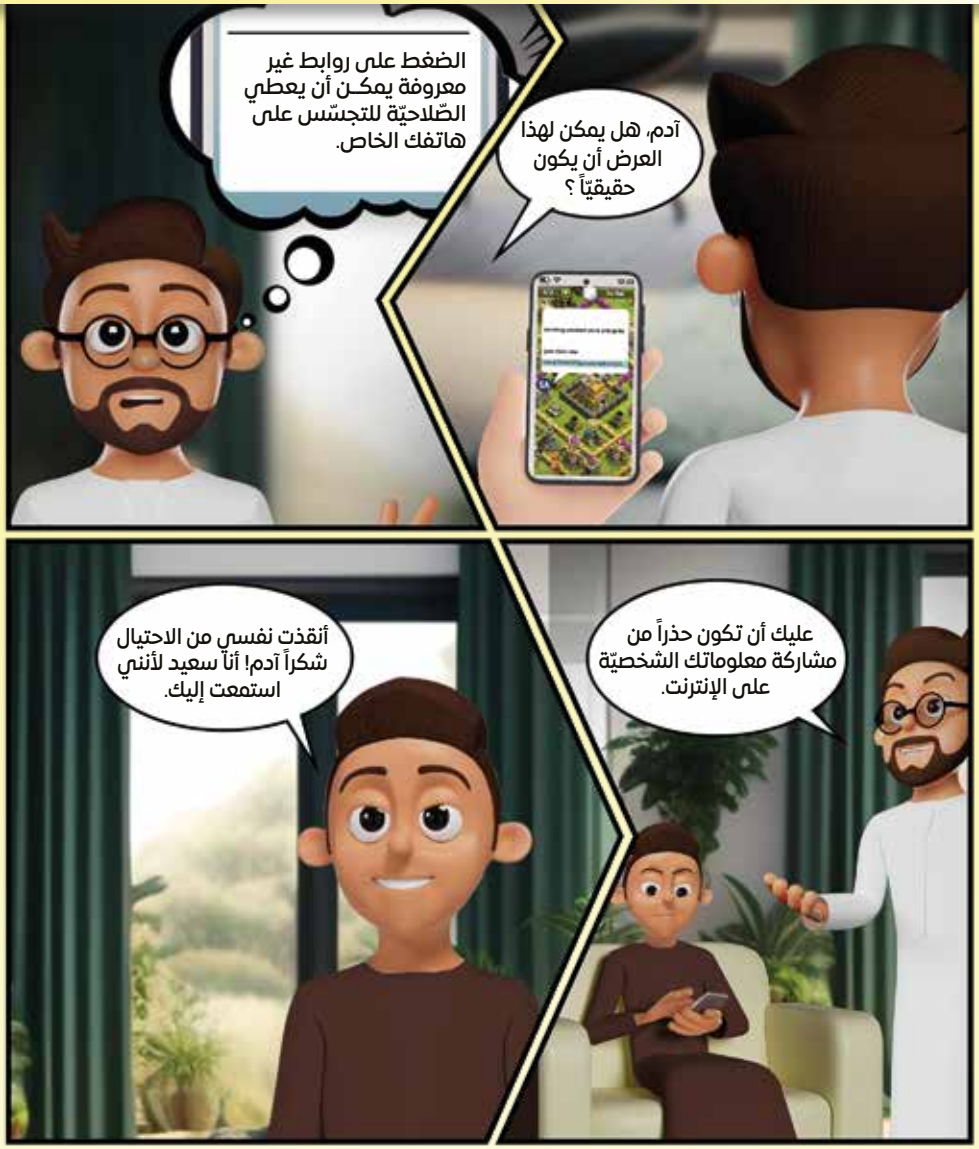
الإعلانات المزيّفة





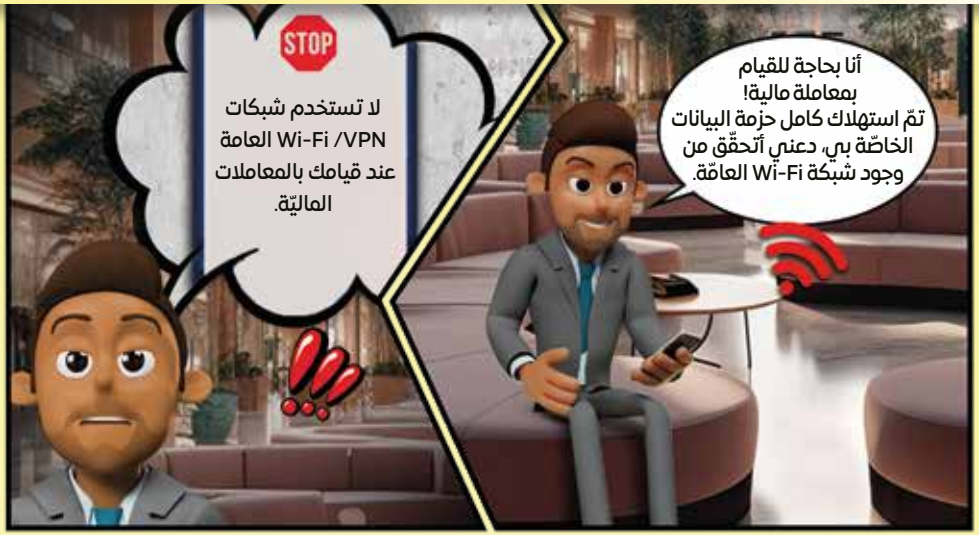
- لا تقم بالضغط على أي روابط لعروض ترويجية أو تخفيضات قد تبدو غير واقعية.
- تواصل مع المعلنين عبر الانترنت عن طريق أرقام رسميّة.
- تأكّد من صحّة الإعلانات عبر مواقع التواصل الاجتماعيّ وبالأخص تلك التي تبدو أفضل من الواقع.
- ابقَ متيقّظ ولا تقع ضحيّة للإعلانات المزيّفة.

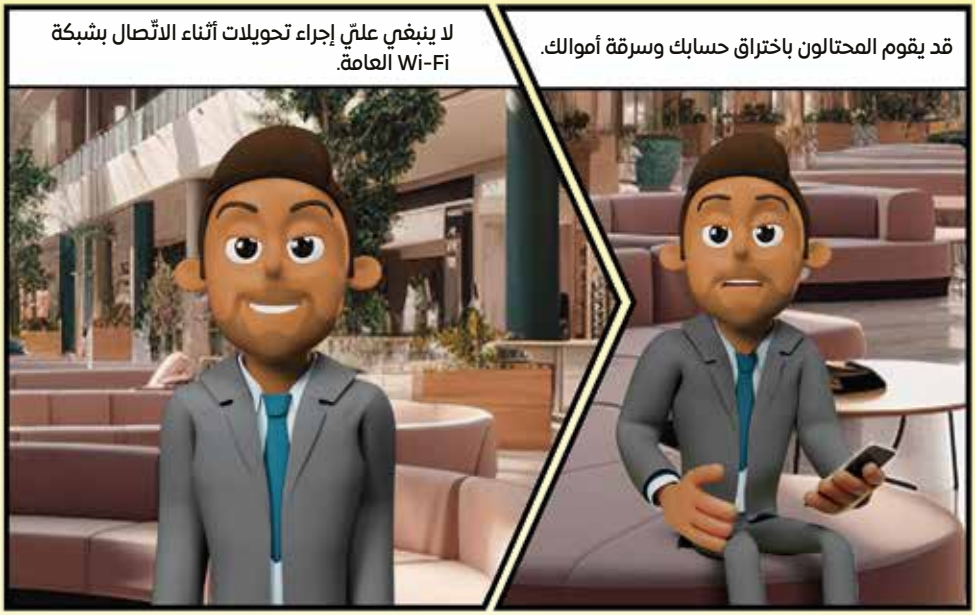
الاحتيال عن طريق الألعاب



- كن حذراً بشأن مشاركة المعلومات الشخصيّة مع الغرباء عبر الإنترنت.
- لا تنقر على الروابط المشبوهة التي يرسلها أشخاص مجهولون.
- عزّز من ثقافتك وثقافة أحبّائك حول إجراءات الحماية عبر الإنترنت.

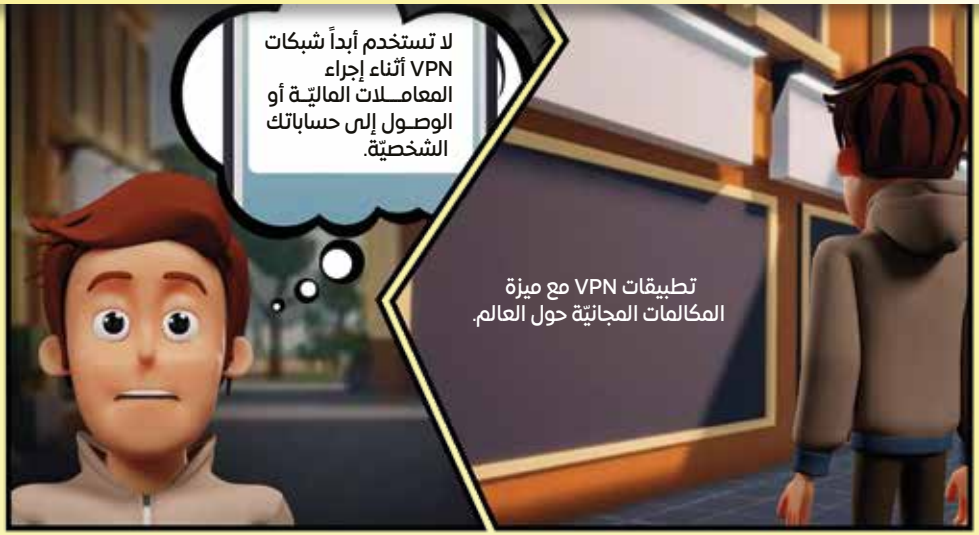
الاحتيال عن طريق شبكات الإنترنت العامّة

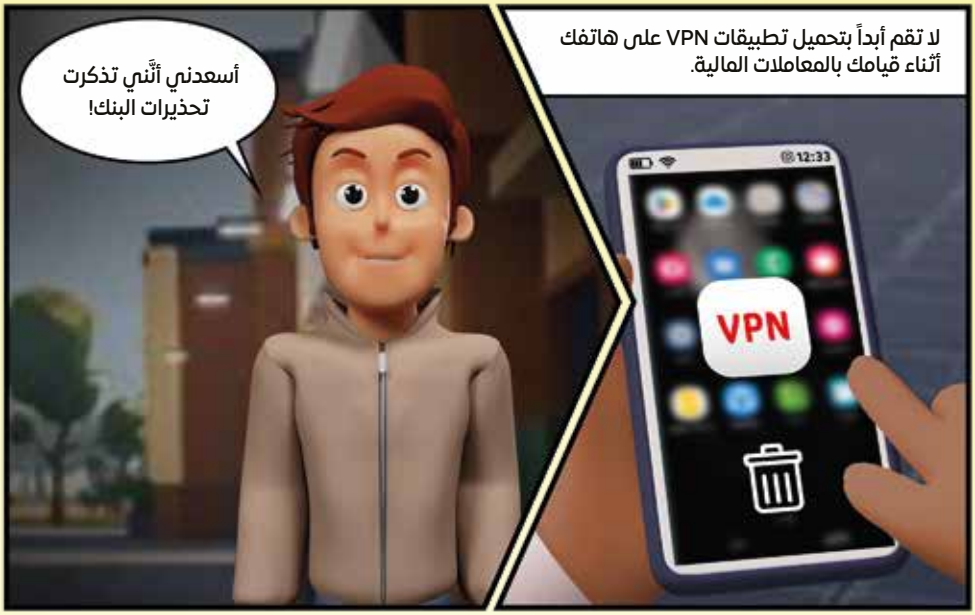




- هناك العديد من المخاطر المرتبطة باستخدام شبكة Wi-Fi العامّة.
- يمكن للمحتالين إجراء المعاملات الماليّة عبر شبكات Wi-Fi العامّة.
- قد يستخدم المحتالون الشبكات العامة لمحاولة إختراق هاتفك والوصول لمعلوماتك الشخصية والبنكية.

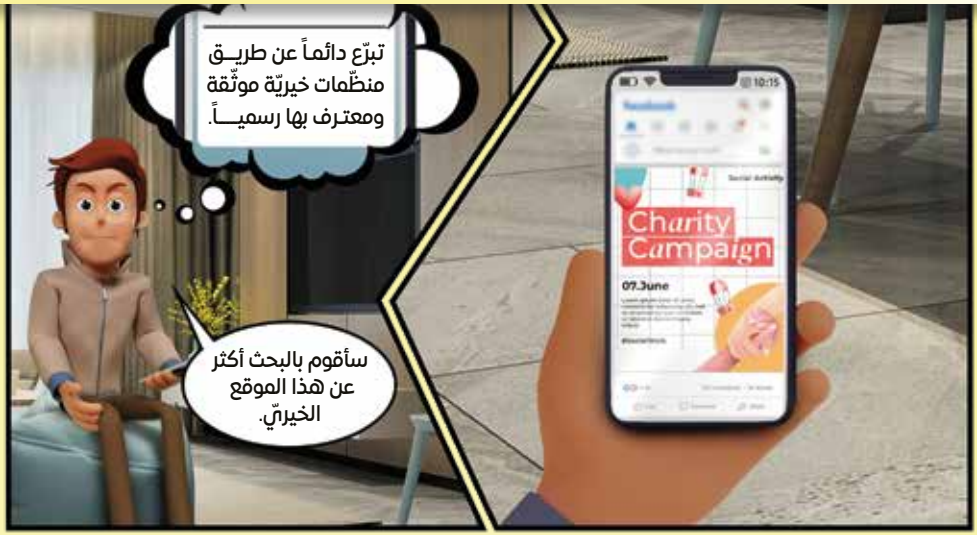
الاحتيال عن طريق تطبيقات الـ VPN

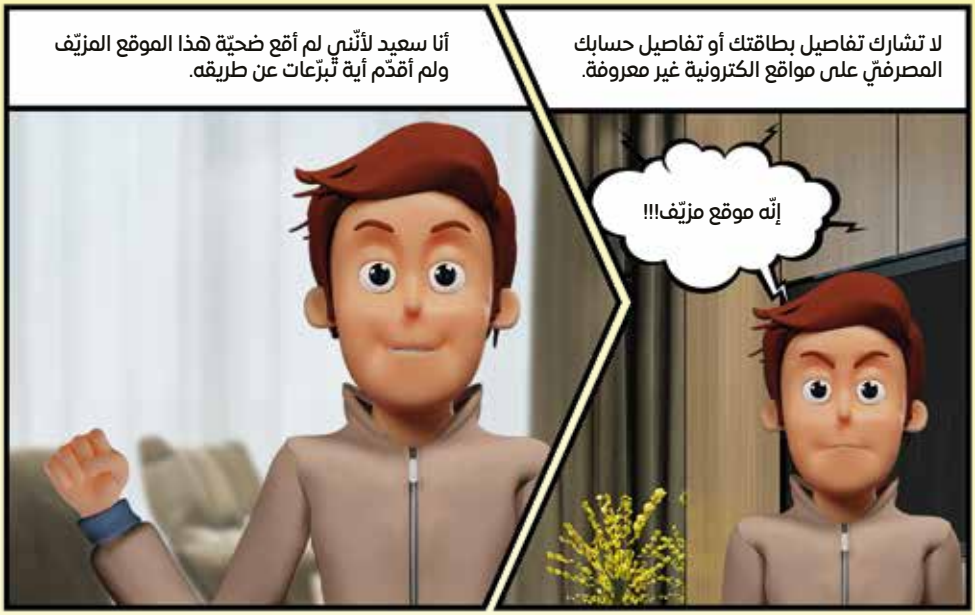




- احذر من تحميل تطبيقات VPN لإجراء معاملات بنكية، لأنها قد تعرّض الخصوصيّة والأمان للخطر.
- من المهم الاتصال بالبنك على الفور لحظر البطاقة في حالة المعاملات المشبوهة والتغيير المتكرّر لبيانات اعتماد تسجيل الدّخول.
- لتتجنب الاختراق، لا تستخدم عنوان البريد الإلكترونيّ نفسه لتلقّي البيانات المصرفيّة والتّسجيل على منصّات مختلفة عبر الإنترنت.

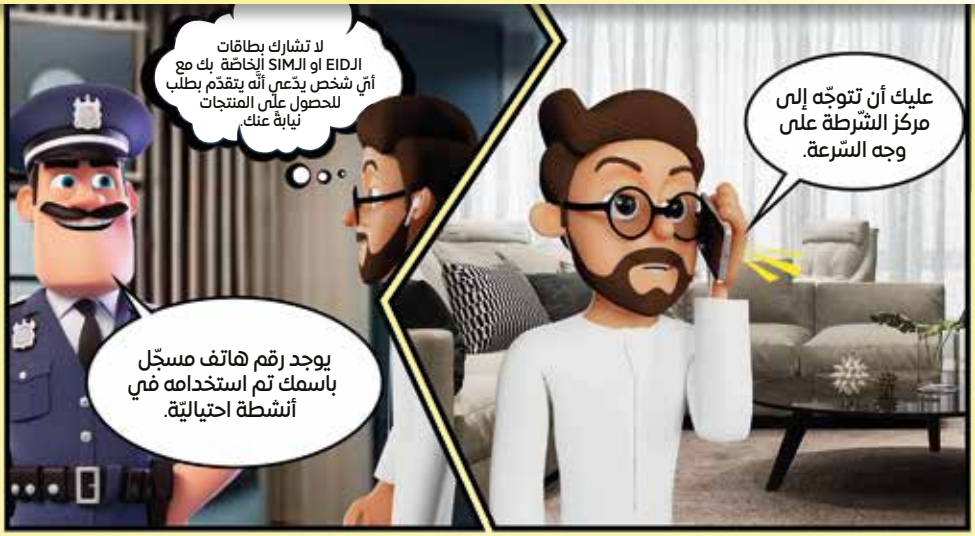
إعلانات الأعمال الخيريّة المشبوهة

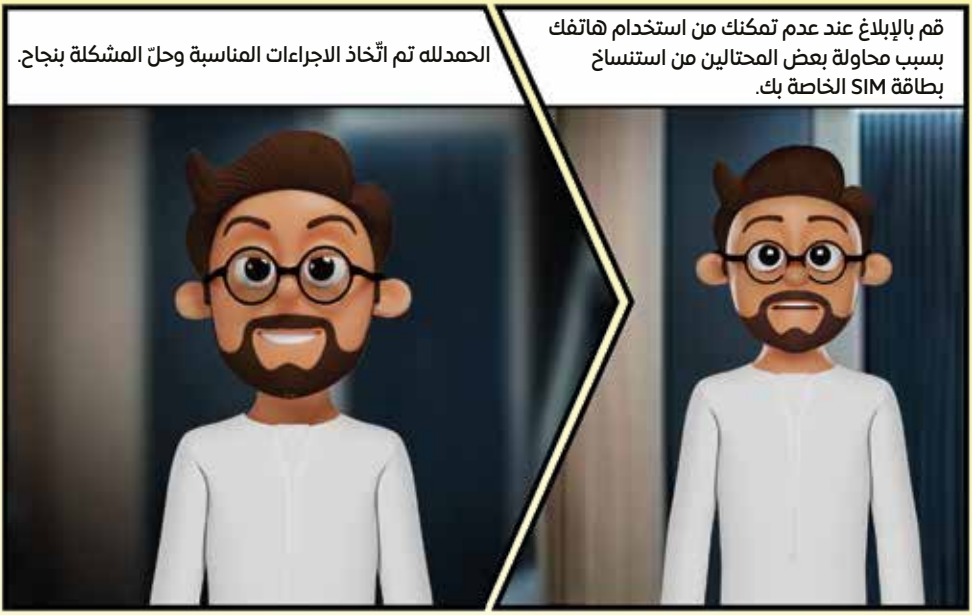




- من المهم التّحقق ممّا إذا كانت المنظّمات الخيريّة موثّقة رسمياً أم لا.
- عليك تقييم صحّة الإعلانات، عن طريق التّحقّق من الرّوابط.
- عليك الامتناع عن مشاركة تفاصيل البطاقة والحساب المصرفيّ على مواقع الكترونية غير معروفة، أو استخدام خيارات الحفظ التلقائيّ لهذه المعلومات في هذه المواقع.

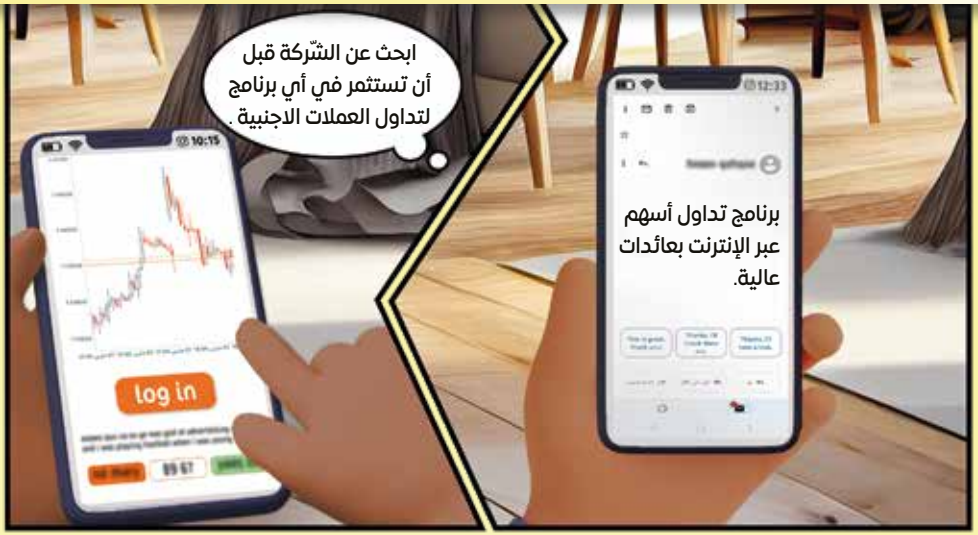
سرقة الهويّة

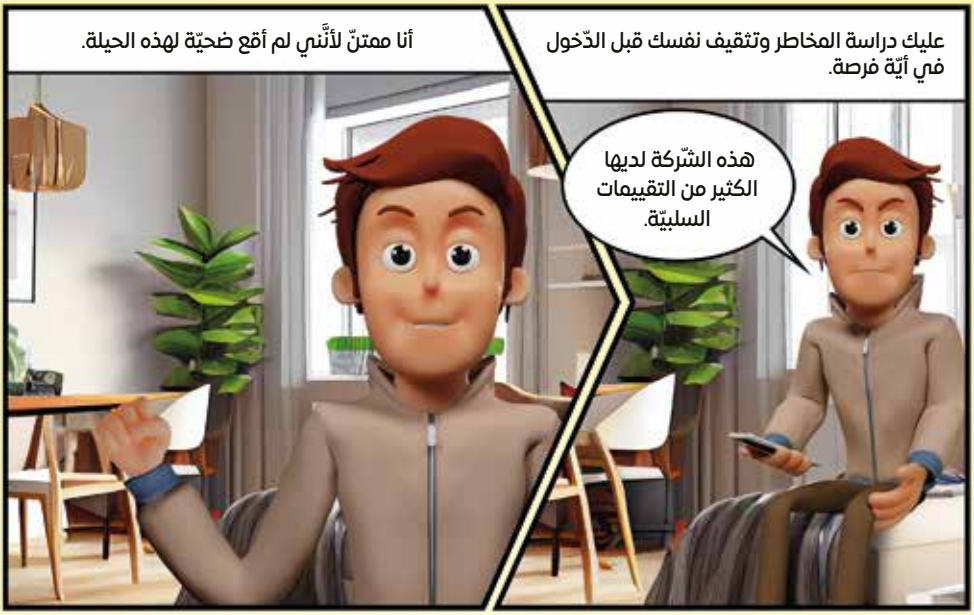




- يعد تبديل بطاقة SIM واستنساخها من الأساليب الّتي يستخدمها المحتالون لاختراق هاتفك المحمول والتحكّم في رقم هاتفك.
- لا تقم بأي نوع من الموافقة الالكترونية التي قد تمكن المحتالون من استنساخ بطاقة SIM الخاصة بك.
- إذا لاحظت أي اختلاف في كشف حسابك البنكي، قم بإبلاغ البنك الذي تتعامل معه على الفور.

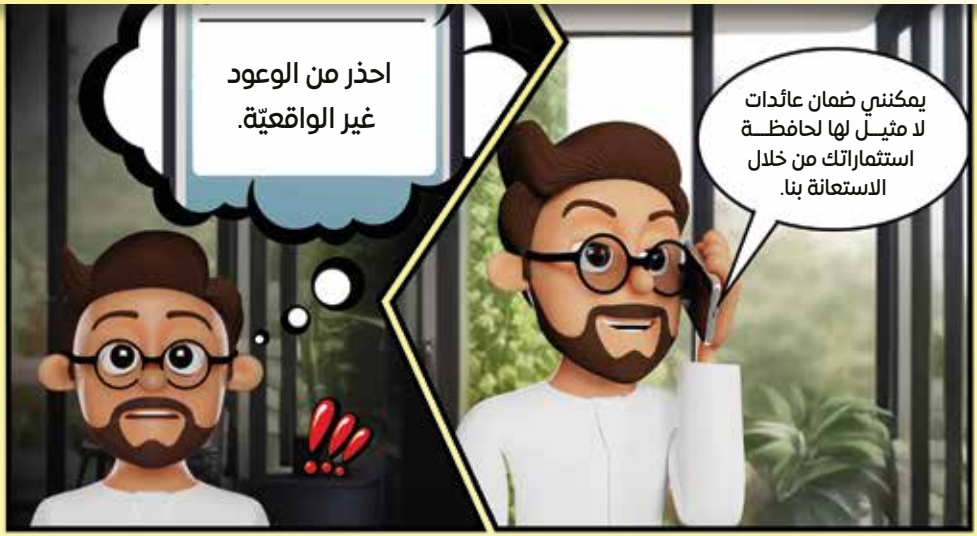
الاحتيال عن طريق منصات تداول العملات الاجنبية والرقمية (FOREX)

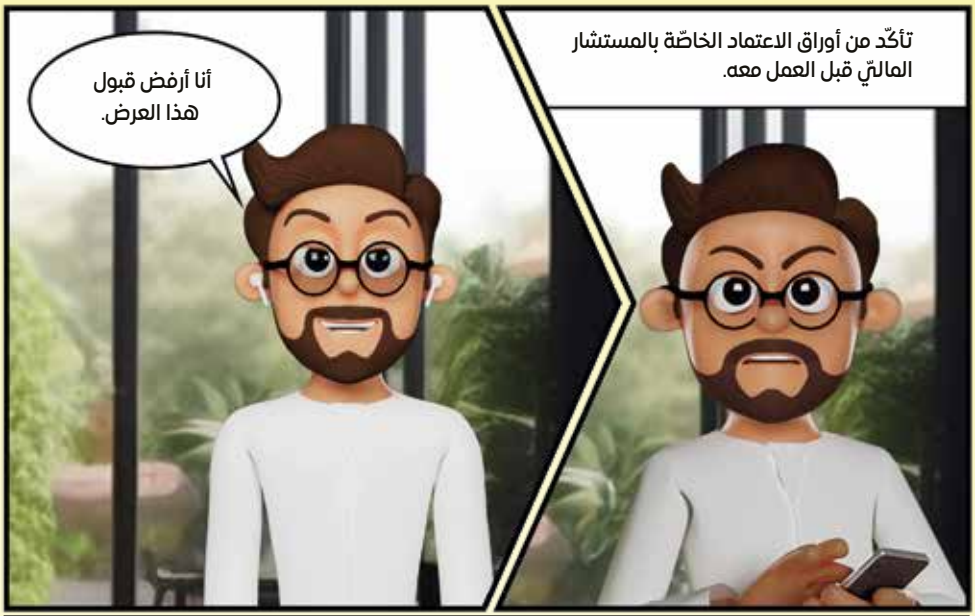




- قم بالبحث دائماً عن الشّركة والوسيط المرخص في الدولة قبل الدّخول في أيّ برنامج تداول عبر الإنترنت.
- احذر من الوعود التي تضمن العائدات المالية، لأنّها غالباً ما تكون طريقة للاحتيال.
- امتنع عن مشاركة تفاصيل الحساب الخاص بك مع أي شخص لضمان أمنك المالي.

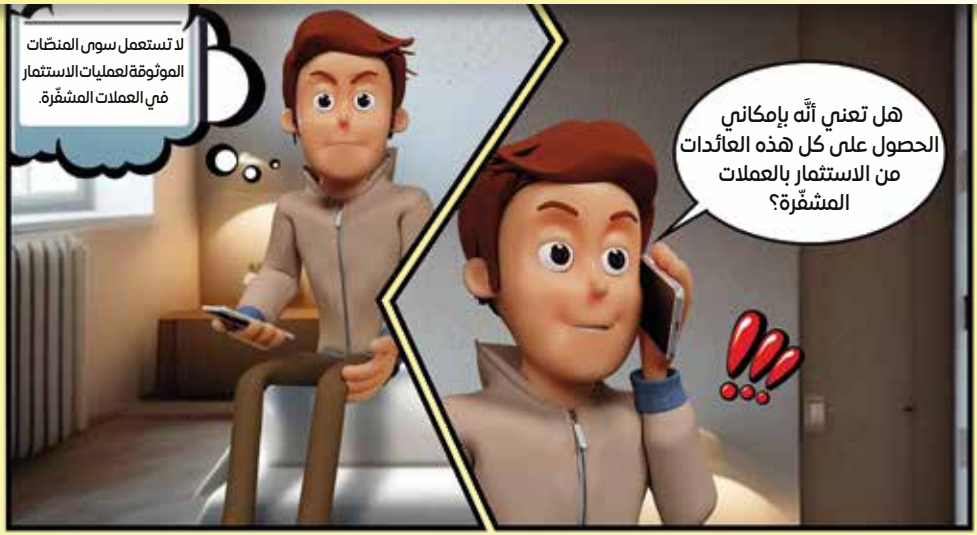
الاحتيال عن طريق حافظة الاستثمارات

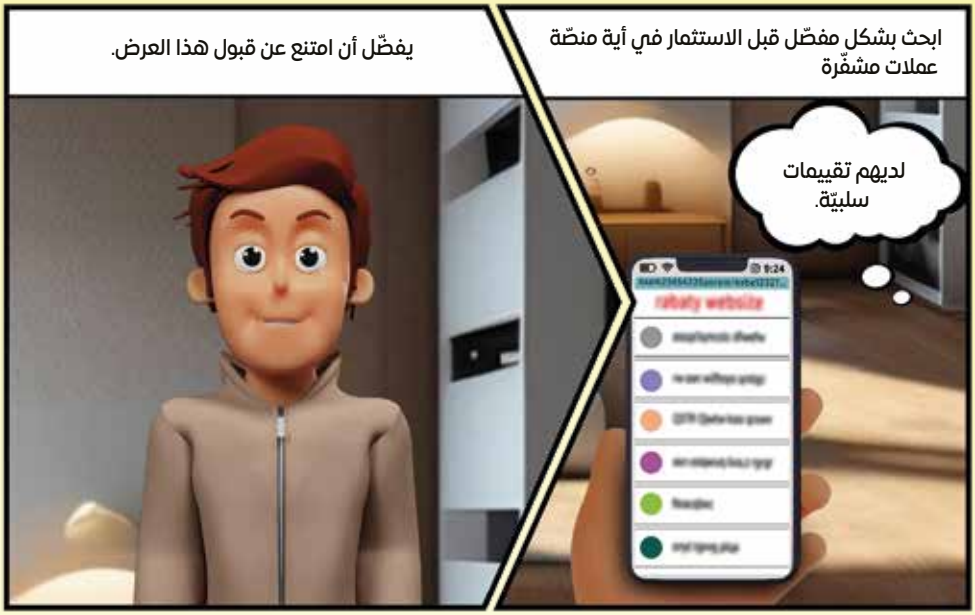




- تأكّد من أوراق الاعتماد والتّرخيص قبل التّعامل مع أي مستشار ماليّ أو مؤسّسة استثمار.
- تأكّد إذا كان الوسطاء مُسجّلين مع سلطة تنظيميّة ذات صلة وما إذا كان التّرخيص الخاص بهم سارياً للعمل.
- قم بدراسة استراتيجيّة ومخاطر الاستثمار.

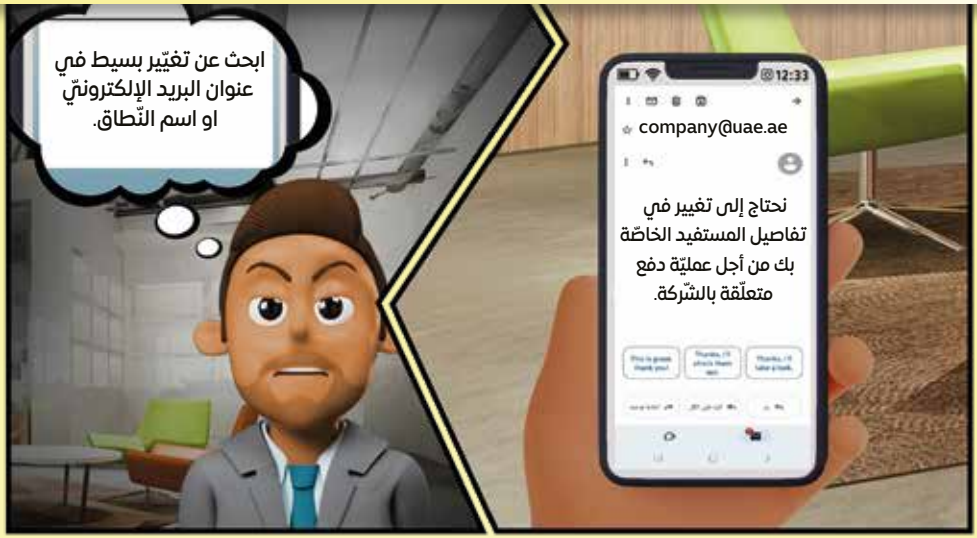
الاحتيال عن طريق العملات المشفّرة

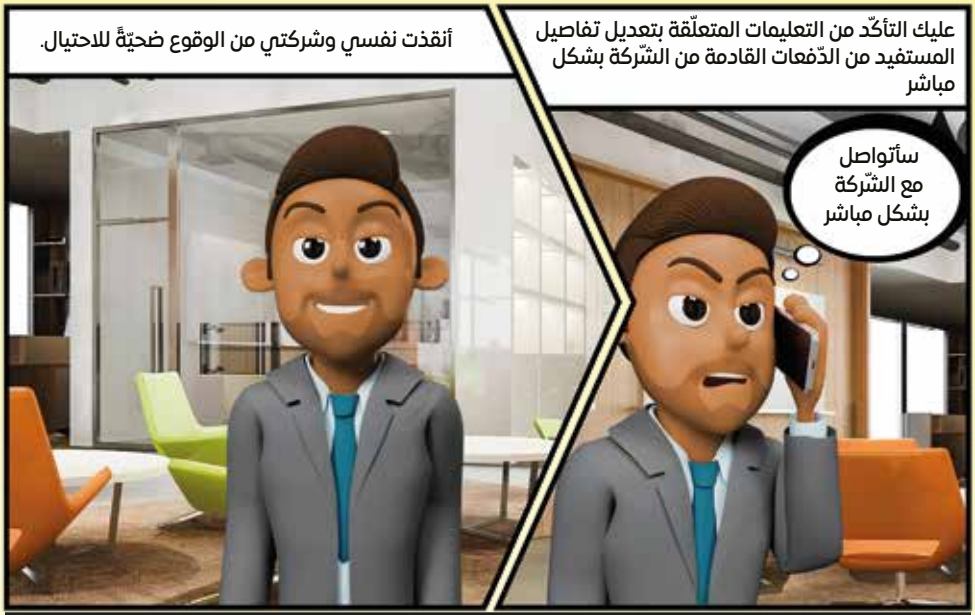




- أظهرت هذه التّجربة أهميّة الشّك في التسويق المبالغ به والعروض التي تبدو أفضل من أن تكون واقعيّة.
- من المهم إقامة بحثاً تفصيليّاً قبل الاستثمار في أيّة عملة مشفّرة.
- احذر من مشاركة بياناتك الشخصيّة أو المعلومات الحسّاسة مع أيّ شخص، وقم بفصل كل من العملات المشفّرة والحسابات البنكيّة.

رسائل البريد الإلكترونيّ المزيّفة

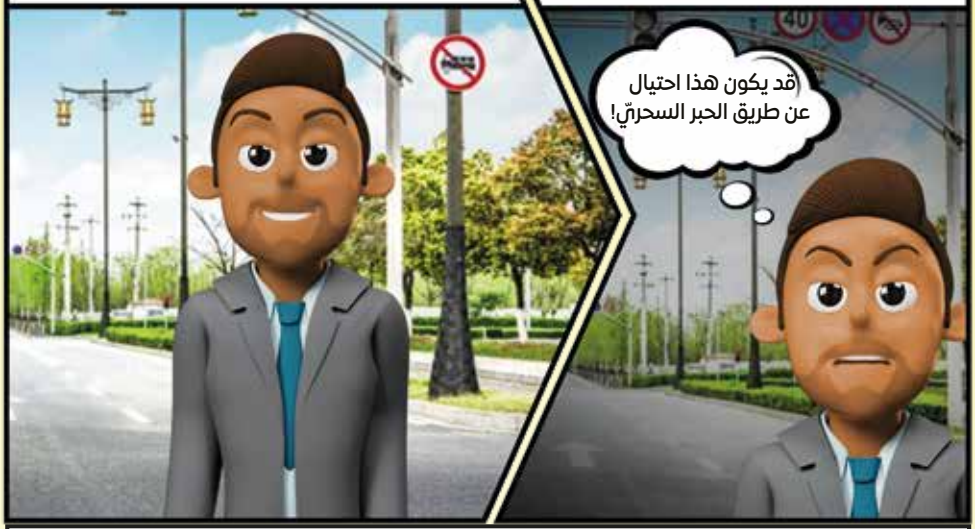




- تأكّد دائماً من تعليمات الدّفع الّتي تصل عبر البريد الإلكترونيّ أو المكالمات الهاتفيّة.
- تحقّق من أيّة تعليمات مشابهة مع الجّهات المعنيّة. بالأخصّ تلك المتعلّقة بأيّة تغييرات في تفاصيل المستفيد للتحويلات المالية.
- ابحث عن أي اختلاف مهما كان صغيراً في عناوين البريد الإلكترونيّ أو أسماء النّطاق.
- تواصل مع الشركة عند استلام طلب لتغيير حساب المستفيد لحساب أو بنك جديد.

الاحتيال بالحبر السحريّ

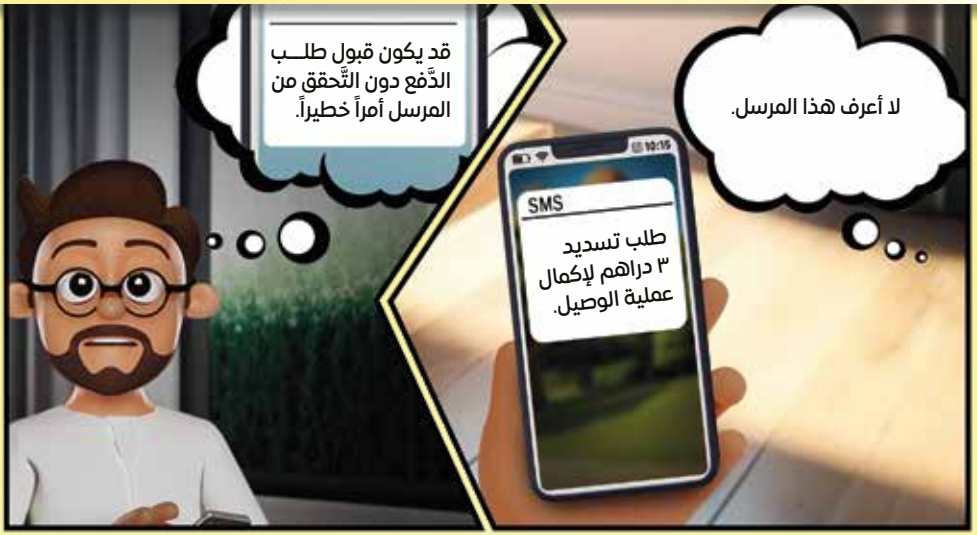
استخدم دائماً قلمك الخاص لملء أي مستندات وطلبات وشيكّات

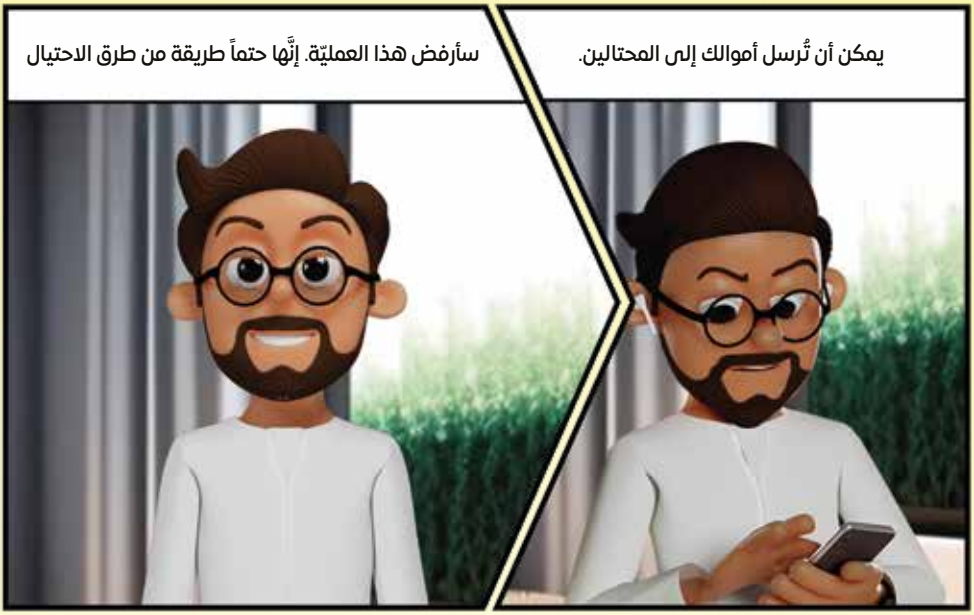


لقد رفضت طلب الوكيل وتجنّبت محاولة الاحتيال.

- اليقظة والوعي الذاتيّ مطلوب جداً في مثل هذه المواقف.
- الحذر مطلوب عند التّعامل مع وكلاء غير مألوفين.
- هناك العديد من المخاطر المرتبطة بممارسات الاحتيال مثل الاحتيال بالحبر السحريّ.

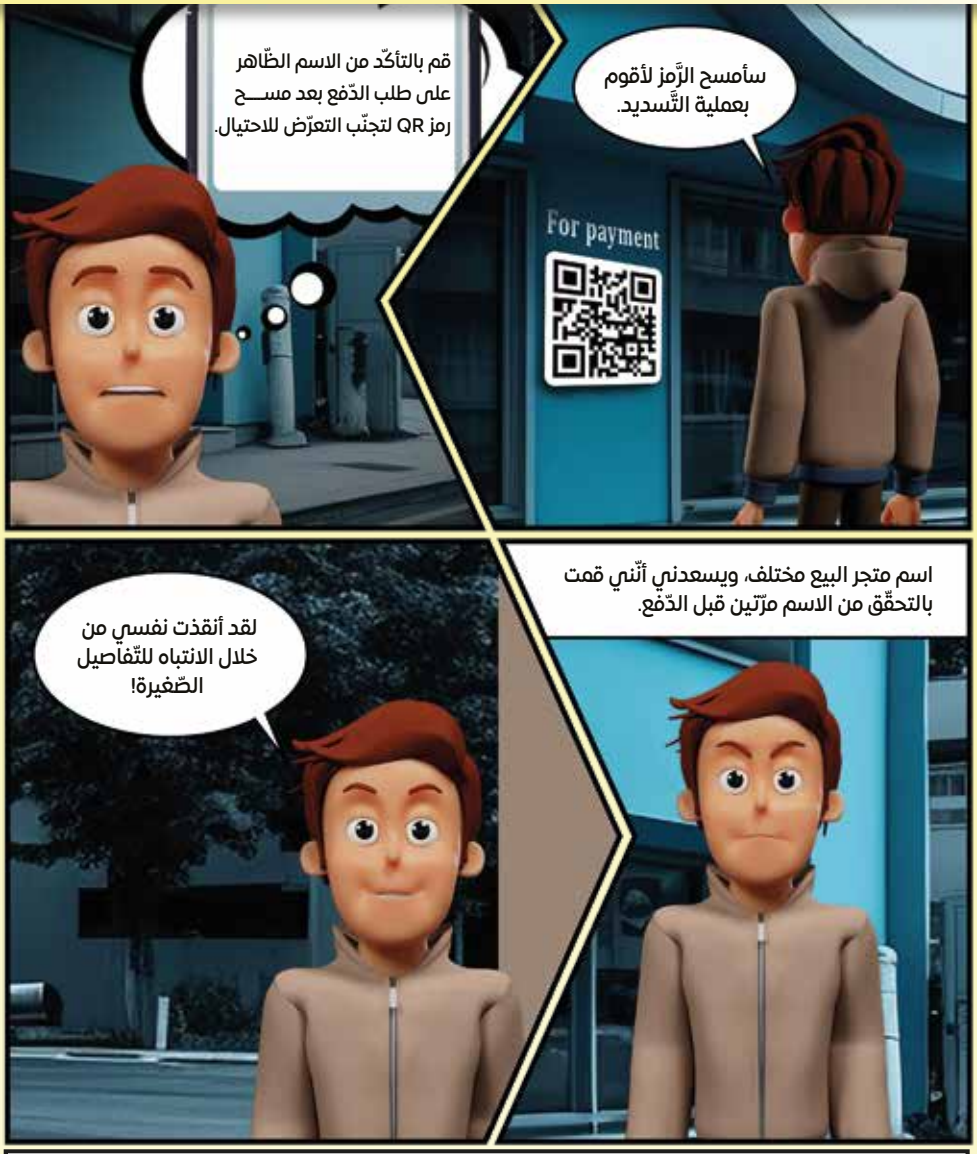
الاحتيال عن طريق طلب الدَّفع





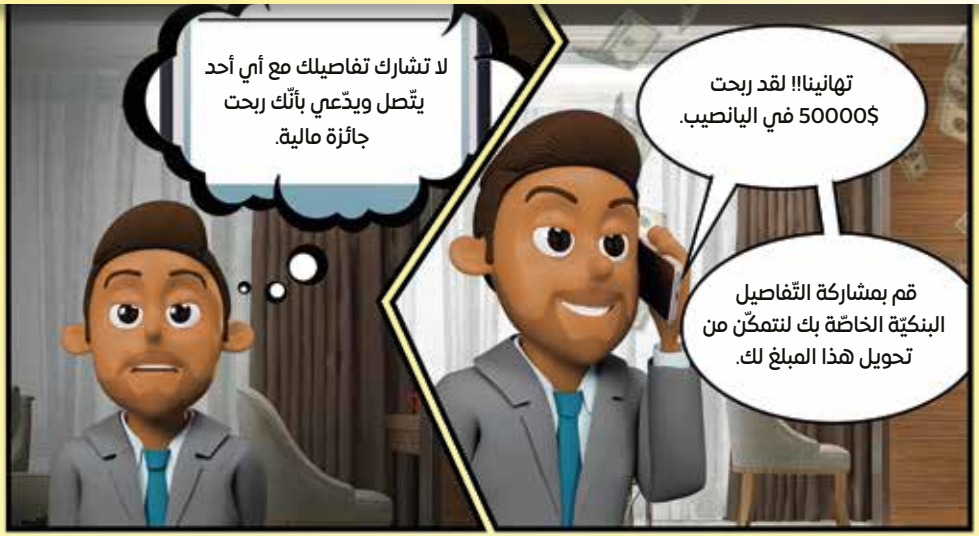
- تحقق مراراً من صحة الرسالة المرسلة قبل الموافقة على الدَّفع.
- التأكد من معلومات المعاملة المالية وقراءة الرسالة المرسلة من البنك قبل إتمام المعامله.

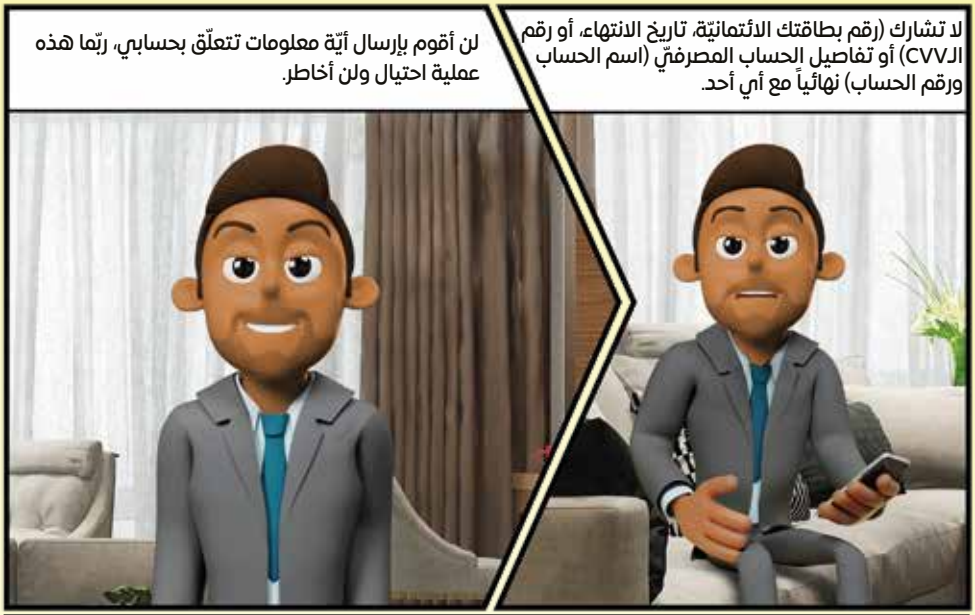
الاحتيال باستخدام الQR



- تحقّق دائماً من اسم متجر البيع بالتّجزئة بعد مسح رمزQR ضوئياً لتجنّب الوقوع بالاحتيال.
- إقرأ الرسالة النصية التي قد تصلك من البنك للتأكد من صحة المعاملة المالية.

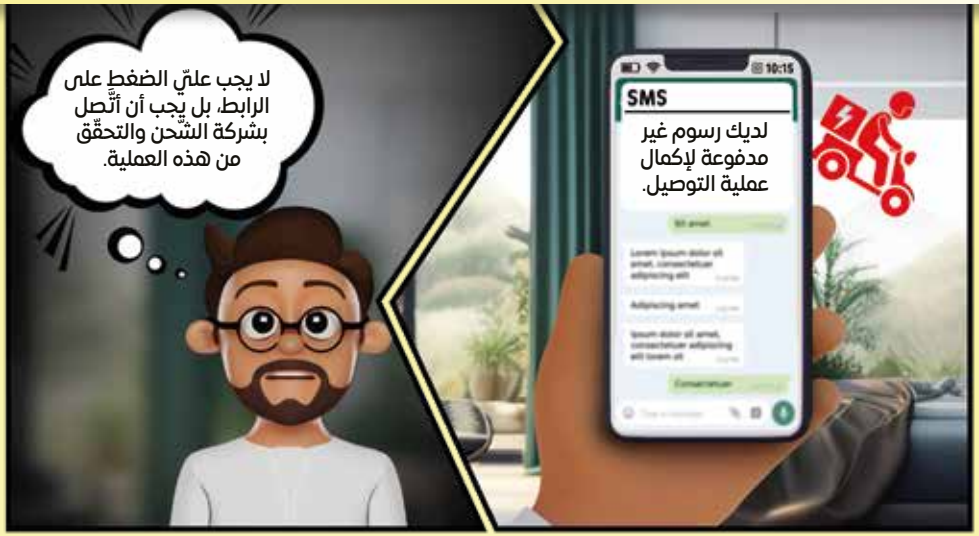
الاحتيال عن طريق الجوائز الوهمية





- لا تشارك (رقم بطاقتك الائتمانيّة، تاريخ الانتهاء، أو رقم الـCVV) أو تفاصيل الحساب المصرفيّ (اسم الحساب ورقم الحساب) نهائياً مع أي أحد.
- قم بالتّبليغ عن المكالمات من مصادر غير معروفة والّتي تُعلمك بجوائز، أو سحب، أو مسابقات.

الاحتيال عن طريق توصيل شركات الشّحن



- لا تنقر على الرّوابط الغريبة نهائيّاً، خاصّة تلك الّتي تتضمّن معلومات ماليّة.
- التحقق من شركة الشحن والإبلاغ إلى السلطات المعنية في حالات الاشتباه بالاحتيال الخاصة بها.
- تأكد من قراءة الرسائل التي قد تصلك من البنك في حال سداد أي رسوم.

اتحاد مصارف الإمارات
UAE BANKS FEDERATION