

سلسلة آدم للوفاية من الاحتيال



تم إعداد هذا الكتيب لمساعدتك في التعرف على أنشطة الاحتيال المحتملة وكيفية مواجهتها. ننصحك بشدة بتصفح هذا الكتيب بتمعن لتكون على دراية بالإجراءات الاستباقية الموضحة لتحمي نفسك من الوقوع ضحية للاحتيال.



حافظت على أموالني بعدم الضغط على الرّابط !!

لا تقم بفتح الروابط التي تصلك عن طريق البريد الإلكترونيّ أو مواقع التّواصل الاجتماعيّ من مصادر غير موثوقة وذلك لتجنّب مخاطر الاحتيال.



تجنّب الصفقات والعروض المغرية التي تكاد لا تصدق.

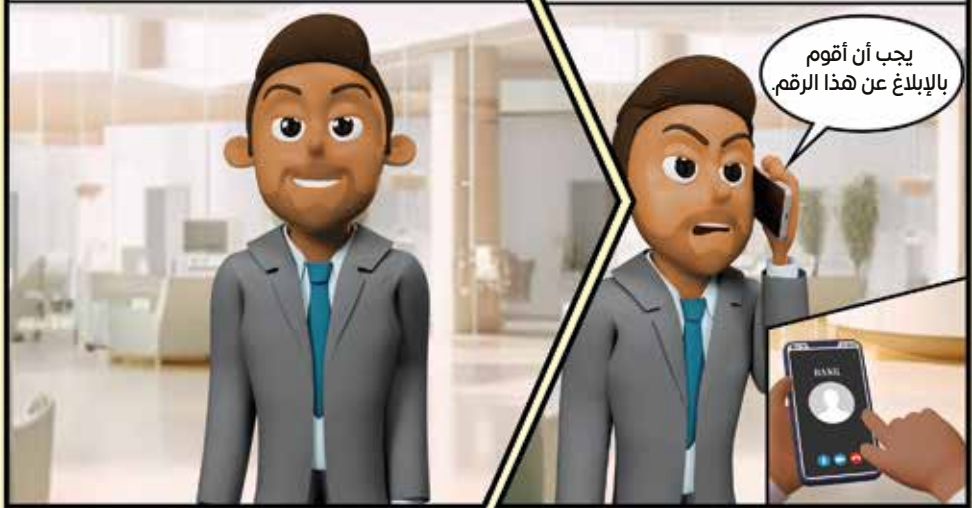
لا تضغط على الرّوابط الواردة عبر رسائل البريد الإلكترونيّ/الرسائل النصية /وسائل التّواصل الاجتماعيّ من مصادر غير موثوقة.

قم دائماً بالتحقّق من العروض من خلال القنوات الرسميّة للمتاجر.



شعر آدم بالارتياح لأنه لم يقع في فخ عملية الاحتيال.

لا تشارك تفاصيل حسابك البنكي الخاص برقم بطاقتك مع أي شخص يتظاهر بأنه يتصل بك من البنك.



- لا تشارك (رقم البطاقة أو تاريخ انتهاء الصلاحية أو رقم CVV) أو تفاصيل حسابك المصرفي (اسم الحساب ورقم الحساب) مع أي شخص يتظاهر بأنه يتصل بك من البنك/السلطات/الشرطة.
- قم بالإبلاغ عن مثل هذه المكالمات إلى الشرطة/ البنك الذي تتعامل معه.
- لن تطلب البنوك أو السلطات أبداً معلوماتك الخاصة أثناء المكالمات الهاتفية.



- كن حذراً عند الضغط على أي رابط تتلقاه خاصة عندما يتعلق الأمر بمعاملات مالية أو تفاصيل شخصية.
- قم بالإبلاغ عن حالات الاحتيال إلى السلطات والتحقق من العروض مباشرة مع البنك.
- تحقق دائماً من مصدر هذه الرسائل.



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

الاحتياط عن طريق منافذ الشحن العمومية



أنا سعيد لأنني تذكرت التحذيرات.

تجنب استخدام الشواحن الموجودة في الأماكن العامة لأنها قد تمكن المحتالين على اختراق جهازك والوصول إلى معلوماتك الشخصية.



تجنب محطات الشحن العامة واستخدم وصلات USB الخاصة بك لاستخدامها في المنافذ الإلكترونية.

قم بالاحتفاظ بشاحن محمول معك للشحن في أي مكان دون اللجوء لاستخدام الشواحن العامة.



أنا سعيد لأنني أنقذت نفسي من الاحتيال.

تجنّب مشاركة تفاصيل بطاقتك الائتمانية عبر وسائل التواصل الاجتماعي ومنصات الانترنت.



■ امتنع عن مشاركة تفاصيل بطاقة ائتمانك عبر مواقع التواصل الاجتماعي، والبريد الإلكتروني، وتطبيقات الرسائل.

■ تذكّر أهمية التأكد من صحة الطلبات المستعجلة التي تصل عبر مواقع التواصل الاجتماعي أو البريد الإلكتروني أو المكالمات الهاتفية.

■ قم بالاتصال هاتفياً للتأكد من صحة الرسائل المرسلة.



أنقذت نفسي من الوقوع في الاحتيال.

لا تقم بدفع أية رسوم مسبقاً لأي شخص يدعي أنه من شركة توظيف.



- فرص العمل التي على الإنترنت قد تكون محاولات إحتيالية.
- على الباحثين عن العمل توخي الحذر فيما يتعلق بالدفع المسبق أو إعطاء معلومات مالية كجزء من استمارة التقديم على العمل.
- يُعد التأكد من صحة فرص العمل أمر أساسي عبر البحث عن حسابات العمل الرسمية أو التواصل المباشر.



اتحاد مصارف الإمارات
UAE BANKS FEDERATION



- ابقَ حذرك عندما يُقدّم لك عروض تبدو رائعة.
- مراجعة وفهم العقود يحميك من التعرّض للاحتيال.
- توجّه الحذر دائماً عند التفكير بالموافقة على أي عرض.



- لا تقم بالضغط على أي روابط لعروض ترويجية أو تخفيضات قد تبدو غير واقعية.
- تواصل مع المعلنين عبر الانترنت عن طريق أرقام رسمية.
- تأكد من صحة الإعلانات عبر مواقع التواصل الاجتماعي وبالأخص تلك التي تبدو أفضل من الواقع.
- ابق متيقظ ولا تقع ضحية للإعلانات المزيّفة.



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

الاحتياال عن طريق شبكات الإنترنت العامة



لا ينبغي علي إجراء تحويلات أثناء الاتصال بشبكة Wi-Fi العامة.

قد يقوم المحتالون باختراق حسابك وسرقة أموالك.



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



- احذر من تحميل تطبيقات VPN لإجراء معاملات بنكية، لأنها قد تعرّض الخصوصية والأمان للخطر.
- من المهم الاتصال بالبنك على الفور لحظر البطاقة في حالة المعاملات المشبوهة والتغيير المتكرّر لبيانات اعتماد تسجيل الدخول.
- لتجنب الاختراق، لا تستخدم عنوان البريد الإلكتروني نفسه لتلقي البيانات المصرفية والتسجيل على منصات مختلفة عبر الإنترنت.



أنا سعيد لأنني لم أقع ضحية هذا الموقع المزيف ولم أقدم أية تبرّعات عن طريقه.

لا تشارك تفاصيل بطاقتك أو تفاصيل حسابك المصرفي على مواقع الكترونية غير معروفة.



■ من المهم التّحقّق ممّا إذا كانت المنظمات الخيرية موثّقة رسمياً أم لا.

■ عليك تقييم صحّة الإعلانات، عن طريق التّحقّق من الرّوابط.

■ عليك الامتناع عن مشاركة تفاصيل البطاقة والحساب المصرفي على مواقع الكترونية غير معروفة، أو استخدام خيارات الحفظ التلقائي لهذه المعلومات في هذه المواقع.



الحمد لله تم اتخاذ الإجراءات المناسبة وحل المشكلة بنجاح.

قم بالإبلاغ عند عدم تمكنك من استخدام هاتفك بسبب محاولة بعض المحتالين من استنساخ بطاقة SIM الخاصة بك.



- يعد تبديل بطاقة SIM واستنساخها من الأساليب التي يستخدمها المحتالون لاختراق هاتفك المحمول والتحكم 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.



- قم بالبحث دائماً عن الشركة والوسيط المرخص في الدولة قبل الدّخول في أي 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.

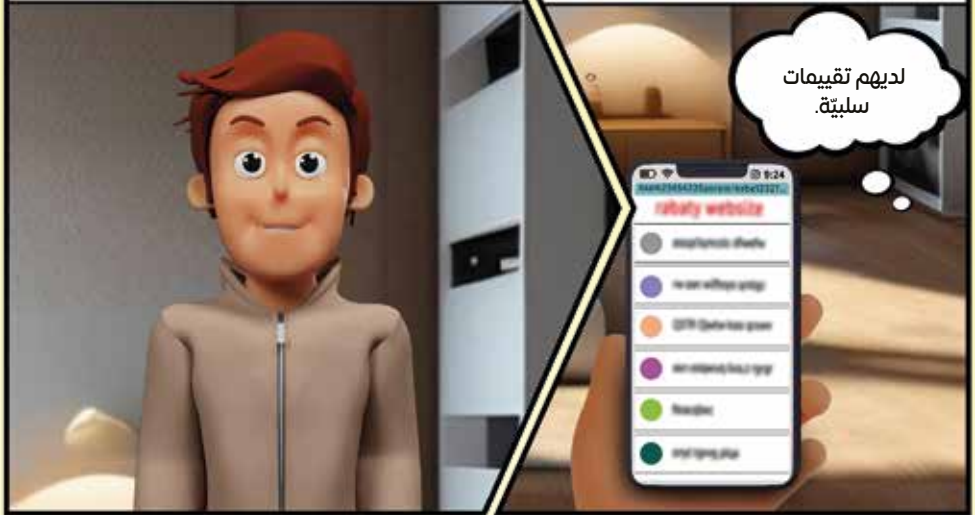


- تأكّد من أوراق الاعتماد والترخيص قبل التعامل مع أي مستشار مالي أو مؤسسة استثمار.
- تأكّد إذا كان الوسيط مُسجّلين مع سلطة تنظيمية ذات صلة وما إذا كان الترخيص الخاص بهم سارياً للعمل.
- قم بدراسة استراتيجية ومخاطر الاستثمار.



يفضّل أن امتنع عن قبول هذا العرض.

ابحث بشكل مفصّل قبل الاستثمار في أية منصة عملات مشفرة



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



أُنقِذت نفسي وشركتي من الوقوع ضحيةً للاحتيال. عليك التأكّد من التعليمات المتعلّقة بتعديل تفاصيل المستفيد من الدفّعات القادمة من الشركة بشكل مباشر



- تأكّد دائماً من تعليمات الدفّع التي تصل عبر البريد الإلكتروني أو المكالمات الهاتفية.
- تحقّق من آية تعليمات مشابهة مع الجهات المعنية، بالأخصّ تلك المتعلّقة بآية تغييرات في تفاصيل المستفيد للتحويلات المالية.
- ابحث عن أي اختلاف مهما كان صغيراً في عناوين البريد الإلكتروني أو أسماء النطاق.
- تواصل مع الشركة عند استلام طلب لتغيير حساب المستفيد لحساب أو بنك جديد.



لقد رفضت طلب الوكيل وتجنبت محاولة الاحتيال.

استخدم دائماً قلمك الخاص لملء أي مستندات وطلبات وشيكات



- البقطة والوعي الذاتي مطلوب جداً في مثل هذه المواقف.
- الحذر مطلوب عند التعامل مع وكلاء غير مألوفين.
- هناك العديد من المخاطر المرتبطة بممارسات الاحتيال مثل الاحتيال بالحبر السحري.



سأرفض هذا العمليّة. إنّها حتماً طريقة من طرق الاحتيال

يمكن أن تُرسل أموالك إلى المحتالين.



■ تحقق مراراً من صحة الرسالة المرسلة قبل الموافقة على الدّفع.

■ التأكّد من معلومات المعاملة المالية وقراءة الرسالة المرسلة من البنك قبل إتمام المعاملة.



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



لن أقوم بإرسال أيّة معلومات تتعلق بحسابي، ربّما هذه عملية احتيال ولن أخاطر.

لا تشارك (رقم بطاقتك الائتمانية، تاريخ الانتهاء، أو رقم الـ CVV) أو تفاصيل الحساب المصرفي (اسم الحساب ورقم الحساب) نهائياً مع أي أحد.



لا تشارك (رقم بطاقتك الائتمانية، تاريخ الانتهاء، أو رقم الـ CVV) أو تفاصيل الحساب المصرفي (اسم الحساب ورقم الحساب) نهائياً مع أي أحد.

قم بالتبليغ عن المكالمات من مصادر غير معروفة والتّي تُعلمك بجوائز، أو سحب، أو مسابقات.



■ لا تنقر على الروابط الغريبة نهائياً، خاصة تلك التي تتضمن معلومات مالية.

■ 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