

كيف تتجنب عمليات الاحتيالالاحتيال

أبدِ علامة تما ِ ه لأنها عملية لحتيا

Arabic

1 يدّعي المحتالون بأنهم ينتمون لمنظمة تعرفها.



عادةً ما يدّعي المحتالون أنهم يتواصلون معك نيابة عن الحكومة. وقد يستخدمون اسمًا حقيقيًا، مثل إدارة الضمان الاجتماعي أو دائرة الإيرادات الداخلية أو نظام الرعاية الطبية أو قد يختلقون اسمًا يبدو رسميًا. ويدّعي بعضهم أنهم يعملون لدى شركة تعرفها، مثل شركة مرافق أو شركة تقنية أو حتى مؤسسة خيرية تطلب تبرعات.

يستخدم المحتالون التكنولوجيا لتغيير رقم الهاتف الذي يظهر لديك في خاصية تحديد هوية المتصل. ولذلك قد يكون الاسم والرقم الظاهران لديك غير حقيقيين.

2 يقول المحتالون إن هناك مشكلة أو جائزة.



قد يقولون إن لديك مشكلة مع الحكومة. أو إنك مدين بالمال. أو إن فردًا من عائلتك لديه حالة طارئة. أو إن هناك فيروسًا على جهاز الكمبيوتر الخاص بك.

يقول بعض المحتالين إن هناك مشكلة في أحد حساباتك وأنهم بحاجة إلى التحقق من بعض المعلومات.

وسيكذب البعض ويقول إنك فزت بجائزة مالية عن طريق القرعة أو جوائز السحب ولكن ينبغي دفع بعض الرسوم للحصول عليها.

3 يحاول المحتالون الضغط عليك لاتخاذ إجراء فورًا.



يريدك المحتالون أن تتخذ قرارك قبل أن تحصل على الوقت الكافي للتفكير. إذا كنت تتواصل معهم عبر الهاتف، فقد يطلبون منك عدم إنهاء المكالمة لكي لا تتمكن من التحقق مما يقولون.

وقد يهددونك بأنك سيُقبض عليك أو ستتم مقاضاتك أوستُسحب رخصة القيادة أو رخصة الأعمال الخاصة بك أو أنه سيتم ترحيلك. وقد يخبرونك بأن جهاز الكمبيوتر الخاص بك على وشك التعطل.

4 يطلب منك المحتالون الدفع بطريقة معينة.



عادة ما يصر المحتالون على الدفع باستخدام العملة المشفرة، عن طريق تحويل الأموال من خلال شركة مثل MoneyGram أو Western Union، أو عن طريق وضع الأموال على بطاقة هدايا ومن ثم إعطاؤهم الأرقام الموجودة على ظهر البطاقة.

سيرسل لك بعضهم شيكًا مصرفيًا (يتبين لاحقًا أنه مزور)، ثم يطلبون منك إيداعه وإرسال المال لهم.

كيف تتجنب عمليات الاحتيال

قم بحظر الاتصالات والرسائل النصية غير المرغوبة.

اتخذ خطوات لحظر الاتصالات غير المرغوبة وأيضًا لتصفية الرسائل النصية غير المرغوبة.

لا تقدم بياناتك الشخصية أو المالية ردًا على طلب لم تتوقعه.

لن تتصل بك المؤسسات الصادقة أو ترسل لك بريدًا إلكترونيًا أو رسالة نصية تطلب منك معلوماتك الشخصية مثل رقم الضمان الاجتماعي أو حسابك البنكي أو أرقام بطاقة الائتمان.

إذا تلقيت بريدًا إلكترونيًا أو رسالة نصية من شركة تقوم بأعمال معها وتعتقد أن هذه الرسالة حقيقية، فيظل من الأفضل عدم النقر على أي روابط. وبدلاً من ذلك، تواصل معهم عبر موقع إلكتروني تعرف أنه موثوق به. أو ابحث عن رقم الهاتف الخاص بهم. لا تتصل برقم أخبروك به أو الرقم الموجود في خاصية تحديد هوية المتصل.

لا تستسلم للضغط باتخاذ إجراء فورًا.

تمنحك المؤسسات الصادقة وقتًا لاتخاذ القرار. أي شخص يضغط عليك للدفع أو لإعطائه معلوماتك الشخصية فهو محتال.

اعرف كيف يطلب منك المحتالون الدفع.

لا تدفع مالاً لأي شخص يصر على أن تدفع له باستخدام العملة المشفرة، أو من خلال خدمة تحويل الأموال مثل Western Union أو MoneyGram، أو باستخدام بطاقة هدايا. ولا تودع أبدًا شيكًا مصرفيًا وترسل مالاً مرة أخرى إلى أي شخص.

توقف للتفكير وتحدث مع شخص تثق به.

قبل فعل أي شيء، أخبر أحد الأشخاص - مثل صديق أو أحد أفراد العائلة أو أحد الجيران - بما حدث. فقد يساعدك التحدث مع أحد الأشخاص على إدراك أن هذه عملية احتيال.

الإبلاغ عن عمليات احتيال إلى FTC

إذا تعرضت للاحتيال أو تظن أنك شاهدت عملية احتيال، فأبلغ FTC على **ReportFraud.ftc.gov**

FEDERAL TRADE COMMISSION

سبتمبر 2022