كيفية تجنب عمليات الاحتيال

أربع علامات دالة على أنها عملية احتيال

Arabic

1 يدّعي المحتالون بأنهم ينتمون لمنظمة تعرفها.

غالبًا ما يدّعي المحتالون بأنهم يتصلون بك نيابة عن الحكومة. وقد يستخدمون اسمًا حقيقيًا، مثل FTC و Social Security Administration (إدارة الضمان الاجتماعي) أو دائرة الإيرادات الداخلية (IRS) أو نظام الرعاية الطبية (Medicare)، أو يختلقون اسمًا يبدو رسميًا. ويدّعي بعضهم أنهم يعملون لدى شركة تعرفها، مثل شركة مرافق أو شركة تقنية، أو حتى مؤسسة خيرية تطلب تبرعات.

يستخدمون التكنولوجيا لتغيير رقم الهاتف الذي يظهر في معرف المتصل لديك. لذلك قد لا يكون الاسم والرقم اللذان يظهران أمامك 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 وإنهم 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 أو ستُسحب 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.

عادةً ما يصر المحتالون على عدم إمكانية الدفع إلا باستخدام العملة المشفرة، وتحويل الأموال من خلال شركة مثل MoneyGram أو Western Union، أو عن طريق تطبيق دفع أو بوضع 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.

كيفية تجنب عمليات الاحتيال

قم بحظر الاتصالات والرسائل النصية غير المرغوبة.

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

لا تقدم بيانات شخصية أو مالية خاصة بك 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 تتعامل معها وتعتقد أنها حقيقية، فلا يزال 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 بالتصرف فورًا.

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

اعرف كيف يطلب منك المحتالون الدفع.

لا تدفع مالاً لأي شخص يصر على أنه لا يمكنك الدفع إلا باستخدام العملة المشفرة، أو من خلال خدمة تحويل الأموال مثل Western Union أو MoneyGram، أو تطبيق دفع أو باستخدام بطاقة هدايا. ولا تقم أبدًا بإيداع شيك وإرسال الأموال إلى شخص ما.

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. يمكن أن يساعدك الحديث عن ذلك على إدراك أنها عملية احتيال.

إبلاغ لجنة التجارة الفيدرالية (FTC) بعمليات الاحتيال

إذا تعرضت إلى عملية احتيال، أو كنت تعتقد أنك رأيت عملية احتيال، فاتصل بالرقم 877-382-4357، ثم اضغط على 3 للغات الأخرى، ثم 5 للغة العربية - أو تفضل بزيارة الموقع **ReportFraud.ftc.gov**.

FEDERAL TRADE COMMISSION

يوليو 2023