حماية أنفسكم من عمليات الاحتيال

الاحتيال هو نشاط غير شريف أو غير قانوني يخدع الناس للتخلي عن المال أو المعلومات الشخصية أو الصور الحميمة أو أي شيء آخر ذي قيمة. عادة ما يتم القيام بعملية احتيال عبر الإنترنت من قبل شخص لديه ملف تعريف مزيف أو شركة وهمية. لذا، بينما يمكن أن يكون الإنترنت مكانًا رائعًا للاستكشاف، إلا أنه من المفيد توخي الحذر!

يُعد التعرّف على المحتالين إحدى الخطوات المهمة لتجنبهم. بمجرد معرفة حيلهم، من المرجح أن تكونوا قادرين على اكتشاف عملية احتيال. البقاء في حالة تأهب هو أفضل دفاع لكم.

إليكم بعض النصائح المهمة للتعرف على عمليات الاحتيال وتجنبها.

حماية معلوماتكم الشخصية

يحاول المحتالون الوصول إلى معلوماتكم الشخصية عن طريق طرح أسئلة عليكم أو إعطاؤكم تعليمات عبر مكالمة هاتفية أو بريد إلكتروني أو رسالة نصية أو عبر وسائل التواصل الاجتماعي. سيستخدم المحتالون تفاصيلكم الشخصية لسرقة أموالكم أو ارتكاب جريمة أخرى.

ماذا يطلب المحتالون؟

يحاول المحتالون كسب ثقتكم من خلال التظاهر بأنهم من منظمة أو وكالة معروفة مثل NBN Co أو Telstra أو Microsoft أو Australia Post أو مكتب الضرائب أو الشرطة أو خدمات أستراليا (MyGov أو Centrelink أو Medicare).

ولخداعكم في التخلي عن معلوماتكم الشخصية أو المالية، قد يقوم المحتالون بما يلي:

- جعلكم تنقرون على رابط
- الطلب منكم منحهم حق الوصول عن بعد إلى جهاز الكمبيوتر الخاص بك
- الطلب منكم دفع دين
- الطلب منكم شراء قسيمة لدفع غرامة
- الطلب منكم تحويل أموال أو إرسال أموال إلى الخارج

علامات على أنها قد تكون عملية احتيال

احذروا من:

- رسائل البريد الإلكتروني أو الرسائل النصية أو المكالمات غير المتوقعة أو من شخص لا تعرفونه
- وعود بفائدة مالية
- تهديدات بغرامة أو دين
- تهديدات لإغلاق أو قَفل حسابكم
- الروابط التي لا تبدو أصلية، مثل امتلاك عنوان موقع غير معتاد
- شعور غير عادي بالإلحاح أو الموعد النهائي

نصيحة: إذا لم تكونوا متأكدين عما إذا كانت الرسالة النصية أو المكالمة حقيقية، فلا تستخدموا تفاصيل الاتصال المقدمة، وبدلاً من ذلك ابحثوا عبر الإنترنت عن رقم المؤسسة أو عنوان البريد الإلكتروني.

كونوا حذرين من الأصدقاء الذين قمتم بتكوينهم عبر الإنترنت

غالبًا ما يتواصل المحتالون عبر الإنترنت مع الأشخاص من خلال وسائل التواصل الاجتماعي. يستخدمون تكتيكاتهم في الحيل الرومانسية أو المواعدة. كما أنهم يستهدفون الأشخاص الذين يلعبون ألعابًا عبر الإنترنت مثل Words with Friends و Scrabble. وهدفهم هو بناء علاقة (ليس بالضرورة أن تكون رومانسية) لكسب ثقتكم حتى يتمكنوا من طلب المال أو المعلومات الشخصية أو الصور الحميمة أو أي شيء آخر ذي قيمة.

علامات على أنها قد تكون عملية احتيال

ابحثوا عن الأشخاص الذين:

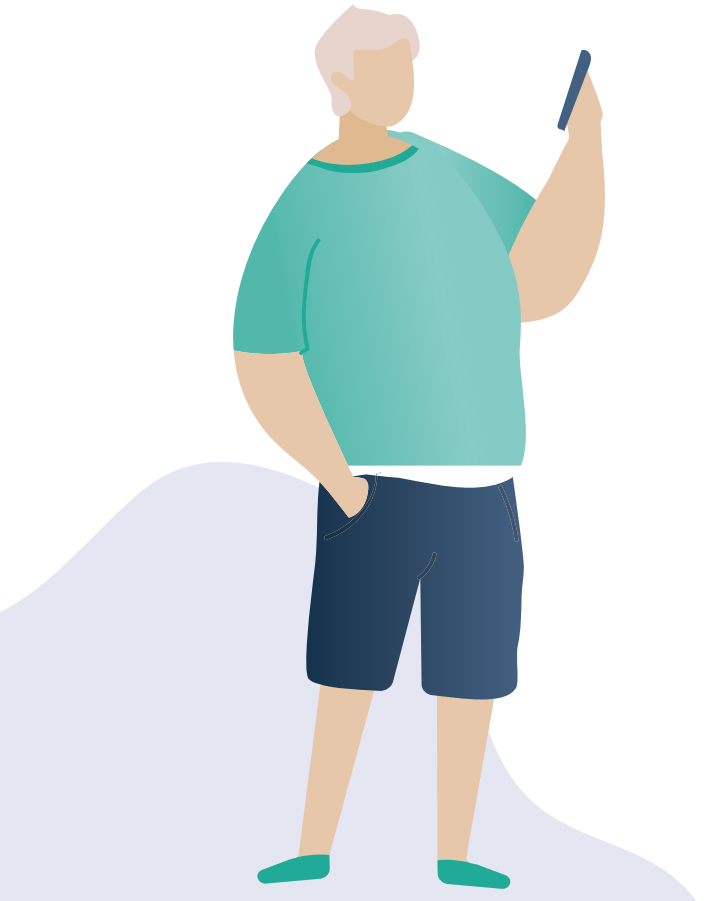
- يعبّرون عن المودة العميقة بسرعة
- يحاولون نقل محادثتكم من موقع الويب الذي التقيتم فيه إلى قناة اتصال أكثر خصوصية، مثل المراسلة المباشرة أو بالبريد الإلكتروني
- يخبروكم قصص مفصلة عن المشاكل المالية
- يقولون أنهم يرغبون في الالتقاء بكم ولكنهم يقدمون الأعذار، أو يطلبون المال حتى يتمكنوا من "السفر" لمقابلتكم
- يسألون عن وضعكم المالي
- يصبحون مصرّين، أو أكثر مباشرة، أو حتى عدوانيين عندما لا ترسلون الأموال
- يبدو أن هناك تناقضات في ملفهم الشخصي عبر الإنترنت - على سبيل المثال، تبدو صورتهم مختلفة عن وصفهم، أو يقولون أنهم متعلمون جامعيون ولكن قواعدهم ضعيفة

من الشائع أيضًا أن يتظاهر المحتالون كعمال إغاثة أو يتظاهرون بأنهم أفراد عسكريون أو محترفون يعملون في الخارج.

نصيحة: أجروا بحثًا على الصور في بعض المواقع مثل Google (images.google.com) أو Tineye (tineye.com)، لمساعدتكم على التحقق عما إذا كان الشخص هو نفسه الذي يقول بأنه هو.

كيف تحمون أنفسكم

- لا تقدموا معلومات شخصية أو مالية لأشخاص لم تلتقوا بهم شخصيًا من قبل.
- لا تسددوا أي دفعات عن طريق حوالة بريدية أو تحويل إلكتروني أو تحويل أموال دولي أو عملة إلكترونية مثل بيتكوين. (من الصعب استرداد الأموال المرسلة بهذه الطريقة، إذا اتضح أنها عملية احتيال.)
- لا توافقوا على حمل الطرود دوليًا أو تحويل أموال لشخص آخر، لأنكم قد ترتكبون جريمة دون علمكم بها.
- لا تشاركوا الصور الحميمة أو تستخدموا كاميرات الويب في مكان حميم.
- أوقفوا كل الاتصالات إذا بدأ شخص يطلب منكم خدمة أو مالاً.
- كونوا منتبهين للأخطاء الإملائية وقواعد اللغة السيئة والتناقضات في القصص



احترسوا من حيل الاستثمار

يضع المحتالون الاستثماريون الكثير من الوقت والجهد والمال في إنشاء قصص مقنعة ومواقع ويب رائعة وكتيبات لامعة لخداع الأستراليين الأكبر سنًا الذين يتطلعون إلى تنمية "أموالهم" أو مدخراتهم.

كيف يجعلكم المحتالون مهتمين؟

فيما يلي بعض الأساليب التي يستخدمها المحتالون الاستثماريون:

- يوجهونكم إلى موقع ويب وهمي يقدم ادعاءات كاذبة بالاستثمارات ذات الأداء الجيد والعوائد الجيدة.
- ينشرون إعلانًا أو مقالاً على أحد مواقع التواصل الاجتماعي مثل Facebook.
- يرسلون لكم طلب "صديق" على وسائل التواصل الاجتماعي من خلال التظاهر كشخص تعرفونه أو مرتبطين به، من أجل الوصول إلى معلومات ملفكم الشخصي وإرسال عروض مخصصة لكم للاستثمار.

علامات على أنها قد تكون عملية احتيال

- يتصل المحتالون أو يرسلون رسائل عبر البريد الإلكتروني لكم بإصرار.
- ينقلون مكالمتكم على طول الخط - شخص مبتدئ يتحدث إليكم أولاً، ثم يحاول شخص مسؤول إنهاء الصفقة.
- يضغطون عليكم للتصرف بسرعة وإلا ستفوتكم الفرصة.
- يقولون أنهم ليس لديهم ترخيص من الخدمات المالية الأسترالية (AFS) أو أنهم لا يحتاجون إلى ترخيص
- يحاولون منعكم من الانسحاب من الصفقة.

المعاش التقاعدي

يقدم المحتالون الاستثماريون طرقًا سريعة وسهلة "للإفراج" عن معاشكم التقاعدي في وقت مبكر. قد يطلبون منكم الموافقة على قصة لضمان الإفراج المبكر عن أموالكم، وبعد ذلك، يتصرفون بصفتهم مستشاركم المالي، ويخدعون شركة التقاعد الخاصة بكم لدفع مخصصات معاشكم التقاعدي مباشرة لهم.

وبمجرد حصولهم على أموالكم، قد يأخذ المحتالون "رسومًا" كبيرة من الأموال المفرجة عنها أو لا يتركون لكم شيئاً على الإطلاق.

ملاحظة! عادة لا يمكنكم الوصول بشكل قانوني إلى الجزء المحفوظ من معاشكم التقاعدي حتى يصبح عمركم بين 55 و 60 عامًا، اعتمادًا على السنة التي ولدتم فيها. هناك بعض الاستثناءات مثل الصعوبات المالية الشديدة أو الأسباب الرحيمة - لكن أي شخص يقدم الوصول المبكر إلى معاشكم التقاعدي يتصرف بشكل غير قانوني.

تضخيم سعر الأسهم بشكل مصطنع

يشتري المحتالون الاستثماريون أسهماً في شركة صغيرة بسعر منخفض، ثم يرسلون نصائح خاطئة عن الشركة بأنها تتمتع بآفاق كبيرة. ومع زيادة عدد الأشخاص الذين يستثمرون، يرتفع سعر السهم ويبيع المحتالون أسهمهم في ذروة ارتفاع السعر. ثم ينخفض سعر السهم ويُترك المساهمون يحتفظون بها بقيمة مخفضة.

عمليات الاحتيال بتأييد من المشاهير

يستخدم المحتالون الاستثماريون موافقات وهمية من رجال أعمال أو مشاهير ناجحين ومحترمين في محاولة لجذب الناس إلى الاعتقاد بأن المشروع مدعوم من قبل شخص يثقون به. غالبًا ما تظهر عمليات الاحتيال هذه كإعلانات عبر الإنترنت أو قصص ترويجية على موجزات وسائل التواصل الاجتماعي أو مواقع ويب تبدو جديرة بالثقة وقانونية.

كيف تحمون أنفسكم

- كونوا حذرين من الفرص التي تبدو جيدة جدًا لدرجة يصعب تصديقها.
- كونوا حذرين من الإعلانات أو القصص المؤيدة من قبل المشاهير.
- لا تدعوا أحدا يضغط عليكم.
- إذا كان عمركم أقل من 55 عامًا، احترسوا من العروض التي تعزز سهولة الوصول إلى مخصصات معاشكم التقاعدي.
- أجروا بحثكم واطلبوا مشورة مالية أو قانونية موثوقة أو مستقلة.
- لا تقدموا معلومات شخصية أو مالية حتى:
  - تحققون عما إذا كان المستشار المالي وشركته مسجلين عبر موقع ASIC asic.gov.au/onlineservices/search-asics-registers/.
  - تراجعون قائمة ASIC للشركات التي يجب ألا تتعاملون معها moneysmart.gov.au/scams/companies-you-should-not-deal-with.

ساعدوني، أظن أنه تم الاحتيال عليّ

إذا كنتم تعتقدون أنكم ضحية لعملية احتيال، فلا تشعروا بالحرج ولا تحتفظوا بها لنفسكم. هناك خطوات يمكنكم اتخاذها لإصلاح المشكلة:

- اتصلوا بالبنك الذي تتعاملون معه وأوقفوا أي دفعات أخرى إلى المحتال
- اتصلوا بـ IDCare idcare.org إذا تم الكشف عن معلوماتكم الشخصية أو إساءة استخدامها.
- بالنسبة لأي خدع Medicare أو Centrelink أو myGov، اتصلوا بـ Services Australia على الرقم 1800 941 126 أو أرسلوا بريدًا إلكترونيًا إلى reportascam@servicesaustralia.gov.au.
- أبلغوا المفوضية الأسترالية للمنافسة والمستهلكين عن عملية الاحتيال على scamwatch.gov.au حتى يتمكنوا من إخبار الآخرين بكيفية تجنبها.

للبقاء على اطلاع بأحدث عمليات الاحتيال التي يجب تجنبها، قوموا بالاشتراك في تنبيهات البريد الإلكتروني الخاصة بـ Scamwatch scamwatch.gov.au/news/subscribe-to-scam-alert-emails

خذوا وقتكم في استكشاف Be Connected

Be Connected هو موقع شامل يحتوي على موارد مجانية مصممة خصيصًا لدعم الأستراليين كبار السن للاتصال عبر الإنترنت بأمان والتنقل في عالم الديجيتل بثقة. هذا الموقع مفيد أيضًا للعائلات والمنظمات المجتمعية التي ترغب في مساعدة أعضاء المجتمع الأكبر سنًا على الوصول إلى جميع مزايا الإنترنت.

beconnected.esafety.gov.au