Be Connected
Every Australian online.

Australian Government

مُلخّص العرض التقديمي عبر الإنترنت

احمِ نفسك من عمليات الاحتيال

يُصبح المحتالون مع الوقت خبراء أكثر فأكثر في محاولاتهم للحصول على أموالك أو تفاصيلك الشخصية. تستهدف عمليات الاحتيال الأشخاص من جميع الخلفيات والأعمار ومستويات الدخل في جميع أنحاء أستراليا. عادةً ما يدير عمليات الاحتيال عبر الإنترنت شخص لديه ملف تعريف مزيّف أو يعمل لشركة مزيّفة أو يتظاهر بأنه من مؤسسة معروفة. لذا، بينما قد يكون من الرائع استكشاف عالم الإنترنت، إلا أنه من المفيد توخي الحذر! كن متيقظاً واحمِ نفسك من الوقوع ضحية لعملية احتيال من خلال اتباع نصائحنا.

احمِ معلوماتك الشخصية

يدّعي المحتالون بأنهم من مؤسسات تعرفها وتثق بها كالشركات التي تتعامل معها أو الوكالات الحكومية أو خدمة مكافحة الاحتيال ويبذلون قصارى جهدهم لحثك على الكشف عن معلوماتك الشخصية والمالية المهمة. قد يتصلون بك عبر مكالمة هاتفية أو عبر وسائل التواصل الاجتماعي أو يرسلون لك رسالة عبر البريد الإلكتروني أو رسالة إلى هاتفك. سيستخدم المحتالون تفاصيلك الشخصية لسرقة أموالك أو ارتكاب جريمة أخرى.

بهدف خداعك لإعطائهم معلوماتك الشخصية أو المالية، قد يطلب المحتالون منك ما يلي:

- إعطائهم معلوماتك الشخصية للتحقق من هويتك أو لتحديث تفاصيلك
- النقر على رابط
- منحهم حق الوصول عن بعد إلى جهاز الكمبيوتر
- دفع دين
- شراء قسيمة شرائية لدفع غرامة
- تحويل الأموال أو إرسال الأموال إلى الخارج.

علامات على أن العملية هي عملية احتيالية

- رسائل عبر البريد الإلكتروني أو الرسائل إلى الهاتف أو المكالمات الهاتفية غير المتوقعة أو من شخص لا تعرفه
- وعود بفائدة مالية
- تهديدات بغرامة أو دين
- تهديدات لإغلاق أو قَفل حسابك
- الروابط التي لا تبدو أصلية، كعنوان موقع إلكتروني غير طبيعي
- شعور غير عادي بالإلحاح أو إعطاء وقت مُحدّد.

تذكّر: قد يحاول المحتالون التلاعب بعواطفك لكي تتفاعل معهم وكي لا تأخذ الوقت الكافي في التفكير ملياً في الموقف. قد يستخدموا التهديدات أو الغرامات، أو يخبرونك بوجود إنفاق غير مُصرّح به من حسابك أو يتظاهرون بأنهم فرد من أفراد العائلة ويحتاجون إلى المساعدة.

كيف تحمي نفسك

- تنبّه إلى حقيقة وجود عمليات الاحتيال وفكّر دائماً في احتمال أن تكون الرسالة أو الرسالة عبر البريد الإلكتروني أو المكالمة الهاتفية هي عملية احتيال.
- اعرف من تتعامل معه. إن لم تكن متأكداً مما إذا كانت الرسالة أو المكالمة حقيقية، فلا تستخدم تفاصيل الاتصال المُقدّمة، وبدلاً من ذلك ابحث عبر الإنترنت عن رقم المؤسسة أو عنوان البريد الإلكتروني.
- لا تقدّم لهم معلوماتك الشخصية أو المالية.
- لا تفتح الرسائل المُريبة أو النوافذ المنبثقة ولا تنقر على روابط أو مرفقات في رسائل البريد الإلكتروني - ما عليك إلا حذفها.
- لا تردّ على المكالمات الهاتفية المتعلقة بجهاز الكمبيوتر من الأشخاص الذين يطلبون منك الوصول عن بُعد إليه - أقفل الخط - حتى لو ذكروا اسم شركة معروفة مثل Telstra.

كن حذراً عند تكوين صداقات عبر الإنترنت

يتصل المحتالون بالأشخاص، عادةً عبر وسائل التواصل الاجتماعي أو مواقع المواعدة أو حتى عبر إحدى الألعاب عبر الإنترنت. ويكونون ودودين للغاية ومثيرين للاهتمام وحريصين على بناء صداقة أو علاقة معك. قد تُفاجأ بالصبر الذي يتحلّى به المحتالون. قد تستمر العلاقة المُزيفة لأسابيع، أو حتى عام حتى يتمكنوا من كسب ثقتك ويطلبوا منك المال أو المعلومات الشخصية أو الصور الحميمة أو خداعك للقيام بشيء غير قانوني.

علامات على أن العملية هي عملية احتيالية

تنبّه للشخص الذين يقوم بما يلي:

- يعبّر عن حبّه العميق لك بسرعة ويتصل بك دائماً
- لا يمكنه الالتقاء بك شخصياً، أو يطلب المال حتى يتمكن من السفر لمقابلتك
- يحاول نقل محادثتكما من المنصة أو التطبيق الذي التقيتما فيه إلى قناة اتصال أكثر خصوصية، مثل المراسلة المباشرة أو تبادل الرسائل عبر البريد الإلكتروني
- يدّعي أنه مستقر من الناحية المالية ولكنه يطلب منك الأموال
- يخبرك قصص مُفصّلة عن مشاكله المالية
- يسألك عن وضعك المالي
- يصبح مستقتلاً للحصول على الأموال أو مُصرّاً أو صريحاً أكثر أو حتى عدوانياً عندما لا ترسل له الأموال
- يبدو أن هناك تناقضات بين قصته وبين ملفه الشخصي عبر الإنترنت - على سبيل المثال، تبدو صورته مختلفة عن وصفه
- يرتكب أخطاء إملائية ونحوية
- يخبرك أنه يعمل خارج أستراليا (على سبيل المثال عامل إغاثة أو يعمل في الجيش).

كيف تحمي نفسك

- لا ترسل أبداً أموالاً أو تُعطي تفاصيل بطاقة الائتمان أو تفاصيل حسابك عبر الإنترنت أو نسخاً من المستندات الشخصية المهمة إلى شخص لم تقابله شخصياً.
- ابحث عن الصور عبر الإنترنت للمساعدة في تحديد ما إذا كان حقاً هو من يدّعي. اذهب إلى images.google.com وانقر على رمز الكاميرا.
- كن حذراً عندما يبدأ في ذكر المشاكل المالية التي يعاني منها أو حاجته إلى المال لحالة طارئة.
- تنبّه للأخطاء الإملائية والنحوية والتناقضات في القصص.
- لا توافق على حمل الطرود دولياً أو تحويل أموال لشخص آخر، لأنك قد ترتكب جريمة جنائية دون علمك بها.
- لا تشارك الصور أو مقاطع الفيديو الحميمة. من المعروف أن المحتالين يبتزون ضحيتهم باستخدام مواد فاضحة.
- اقطع كل الاتصالات إذا بدأ الشخص بطلب الأموال أو المساعدة.
- تجنّب أي ترتيبات مع شخص غريب يطلب منك الدفع عن طريق حوالة بريدية أو تحويل إلكتروني أو تحويل أموال دولي أو بطاقة مُحملة بالأموال مسبقاً أو عملة إلكترونية مثل Bitcoin. من النادر التمكّن من استرداد الأموال المُرسلة بهذه الطريقة.

احترس من عمليات الاحتيال الاستثمارية

تتضمن عمليات الاحتيال الاستثمارية وعود بأرباح عالية وبسرعة وعوائد مضمونة. احذر دائماً من أي فرص استثمارية تَعِدك بعوائد مرتفعة مع مخاطر قليلة أو معدومة.

يخسر الأستراليون أموالاً من عمليات الاحتيال الاستثمارية أكثر من أي عملية احتيال أخرى. قد يكون من الصعب اكتشافها لأن المحتالين يبذلون جهداً كبيراً لخلق قصص مُقنعة وإنشاء مواقع إلكترونية ومواد ترويجية احترافية. قبل الاستثمار، اطلب دائماً المشورة القانونية المستقلة أو النصيحة المالية من مستشار مالي مُسجّل لدى هيئة الأوراق المالية والاستثمارات الأسترالية (ASIC).

إليك بعض الطرق الأكثر شيوعاً التي يستخدمها المحتالون لإجراء عمليات الاحتيال الاستثمارية:

- الاتصال بك عبر البريد الإلكتروني أو الهاتف وإبلاغك عن فرصة مميزة للحصول على عوائد سريعة أو مضمونة
- استخدام المصادقات الزائفة من المشاهير لكي تبدو عملية الاحتيال مشروعة
- إقناعك بالوصول إلى صندوق الادخار التقاعدي مُبكراً أو كامل المبلغ دفعة واحدة
- الندوات الاستثمارية (غالباً عبر الفيديو عبر الإنترنت أو Zoom أو ما شابه) تكون مجانية أو تفرض رسوم حضور عالية.

صندوق الادخار التقاعدي

تطلب منك عملية الاحتيال المُرتبطة بصندوق الادخار التقاعدي الوصول المُبكر إلى حسابك من خلال صندوق للادخار التقاعدي يتمّ إدارته ذاتياً أو مقابل رسوم. قد يأتي العرض من محتال يتظاهر بأنه مستشار مالي.

قد يطلب منك الموافقة على قصة لضمان الإفراج المبكر عن أموالك، وبعد ذلك، من خلال التصرف على أنه مستشارك المالي، يخدع شركة صندوق الادخار التقاعدي التي تتعامل معها لدفع مخصصات معاشك التقاعدي مباشرة له. وبمجرد حصوله على أموالك، قد يأخذ المحتال "رسوماً" عالية من هذه الأموال أو لا يترك لك شيئاً على الإطلاق.

ملاحظة: لا يمكنك عادةً الوصول بشكل قانوني إلى الجزء المحفوظ من معاشك التقاعدي حتى يصبح عمرك بين 55 و 60 عاماً، اعتماداً على السنة التي ولدت فيها. هناك بعض الاستثناءات مثل الصعوبات المالية الشديدة أو الأسباب الرحيمة - لكن أي شخص يقدم طلباً للوصول المُبكر إلى معاشك التقاعدي يتصرّف بشكل غير قانوني. للمزيد من المعلومات يُرجى زيارة الموقع الإلكتروني: moneysmart.gov.au/how-super-works/superannuation-scams

الإعلانات للأسهم والنصائح المهمة

قد يتصل بك المحتالون عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو ينشرون رسالة في أحد المنتديات لتشجيعك على شراء أسهم في شركة يتوقعون أن تزيد قيمتها. تبدو الرسالة وكأنها من طرف داخلي وستشدد عادةً على أنك بحاجة إلى التصرّف بسرعة. يحاول المحتال إقناعك بشراء الأسهم لرفع سعرها حتى يتمكّن من بيع الأسهم التي اشتراها بالفعل لتحقيق ربح هائل. بعدها تنخفض قيمة الأسهم بشكل كبير.

عمليات الاحتيال من خلال مصادقة المشاهير

يستخدم المحتالون صورة المشاهير وأسمائهم وخصائصهم الشخصية دون إذن منهم لإغرائك بالاستثمار لأنه مدعوم من قبل شخص تثق به. غالباً ما تظهر عمليات الاحتيال هذه كإعلانات عبر الإنترنت أو قصص ترويجية على موجزات وسائل التواصل الاجتماعي أو مواقع إلكترونية تبدو جديرة بالثقة وقانونية.

علامات تحذيرية لعملية احتيال استثمارية

يتصل بك فجأة شخص عبر مكالمة هاتفية أو رسالة إلى هاتفك أو بريد إلكتروني أو رسالة عبر وسائل التواصل الاجتماعي يقدّم لك نصائح استثمارية لم تسأله عنها وهو:

- يستخدم أساليب الضغط العالي، بما في ذلك الاتصال بك بشكل مُتكرّر والضغط عليك لاتخاذ قرار بسرعة.
- يَعِدُك بمخاطر منخفضة مع عوائد عالية أو مضمونة.
- ليس لديه ترخيص من الخدمات المالية الأسترالية (AFS) أو أنه لا يحتاج إلى ترخيص.
- لديه أطروحة استثمارية غير مُسجّلة لدى ASIC.
- يستخدم مصادقات أو صور المشاهير: وهي عادةً ما تكون مُزيّفة. من النوادر أن يناقش المشاهير استثماراتهم أو قراراتهم المالية مع العامة.
- يوجّهك إلى موقع إلكتروني مُزيّف.
- يحاول منعك من الانسحاب من الصفقة.

كيف تحمي نفسك

- كن حذراً إذا بدا الأمر جيداً لدرجة قد يصعب تصديقها.
- كن حذراً من الإعلانات أو القصص المُصدّقة من المشاهير.
- لا تسمح لأحد بالضغط عليك.
- إذا كان يقل عمرك عن 55 عاماً، احترس من العروض التي تعزز سهولة وصولك إلى مخصصات معاشك التقاعدي.
- ابحث واطلب المشورة المالية أو القانونية الموثوقة أو المستقلة.
- لا تقدم معلومات شخصية أو مالية حتى:
  - تتحقق عمّا إذا كان المستشار المالي وشركته مُسجلين عبر موقع ASIC الإلكتروني asic.gov.au/online-services/search-asic-s-registers/
  - تُراجع قائمة ASIC للشركات التي يجب ألا تتعامل معها moneysmart.gov.au/companies-you-should-not-deal-with

أهم النصائح لتجنّب عمليات الاحتيال

توقّف

- خذ وقتك قبل إعطاء الأموال أو المعلومات الشخصية لأي شخص.
- سيعرض المحتالون عليك المساعدة أو يطلبون منك المعلومات الشخصية للتحقق من هويتك. سيتظاهرون بأنهم من مؤسسات تعرفها وتثق بها مثل الشركات التي تتعامل معها أو الشرطة أو الحكومة أو خدمة مكافحة الاحتيال.

فكّر

- اسأل نفسك هل يمكن أن تكون الرسالة أو المكالمة مُزيّفة؟
- لا تنقر أبداً على رابط في رسالة واسأل صديقاً أو فرداً من العائلة تثق به عما سيفعله لو كان في مكانك. تواصل فقط مع الشركات أو الهيئات الحكومية باستخدام معلومات الاتصال من مواقعها الإلكترونية الرسمية أو من خلال تطبيقاتها الآمنة. إن لم تكن متأكداً، قل لهم لا، واقفل الخط أو احذف الرسالة.

احمِ

- تصرّف بسرعة إذا شعرت أن هناك شيئاً لا يبدو صائباً.
- اتصل بالبنك الذي تتعامل معه على الفور إذا خسرت أموالاً أو معلومات شخصية أو إذا لاحظت نشاطاً غير عادي على بطاقاتك أو حساباتك. اطلب المساعدة من منظمات مثل IDCARE وأبلغ عن الجريمة عبر الإنترنت إلى ReportCyber. ساعد الآخرين بالإبلاغ عن عمليات الاحتيال إلى Scamwatch.

ساعدوني، أظن أنني وقعتُ ضحية عملية احتيال

إذا كنت تعتقد أنك ضحية لعملية احتيال، فلا تشعر بالحرج ولا تحتفظ بهذا السرّ لنفسك. هناك خطوات يمكنك اتخاذها لحلّ المشكلة

- اتصل بالبنك أو المؤسسة المالية التي تتعامل معها على الفور وأوقف أي دفعات إضافية إلى المحتال.
- إذا وقعت ضحية لجريمة عبر الإنترنت وخسرت أموالاً، فيمكنك إبلاغ الشرطة عن طريق ReportCyber أو زيارة الموقع الإلكتروني: cyber.gov.au
- إذا كنت قلقاً من أنه تمّ الكشف عن معلوماتك الشخصية وإساءة استخدامها، فاتصل بخدمة أستراليا للهوية الوطنية والدعم عبر الإنترنت IDCARE على الرقم 1300 432 273 أو idcare.org
- أبلغ عن عملية الاحتيال إلى ACCC عبر صفحة scamwatch.gov.au/report-a-scam. يساعد هذا في تحذير الأشخاص من عمليات الاحتيال ومراقبة التوجهات الحالية وتعطيل عمليات الاحتيال حيثما أمكن ذلك.
- انشر الخبر لأصدقائك وعائلتك لحمايتهم.

تذكّر: المساعدة متوفّرة دائماً - سواء الأشخاص في cyber.gov.au أو scamwatch.gov.au، أو صديقاً أو أحد أفراد العائلة والذي لديه خبرة في التكنولوجيا، أو حتى نادي كمبيوتر محلي.

للبقاء على اطلاع بأحدث عمليات الاحتيال التي يجب تجنّبها، اشترك في رسائل التنبيه عبر البريد الإلكتروني الخاصة بـ Scamwatch

خذ وقتك في استكشاف Be Connected

Be Connected هو موقع شامل يحتوي على موارد مجانية مصممة خصيصاً لدعم الأستراليين المُسنّين للاتصال عبر الإنترنت بأمان والتنقّل في العالم الرقمي بثقة. هذا الموقع مفيد أيضاً للعائلات والمنظمات المجتمعية التي ترغب في مساعدة أعضاء المجتمع الأكبر سناً على الوصول إلى جميع مزايا الإنترنت.

يُرجى زيارة beconnected.esafety.gov.au

تم تطوير هذا البرنامج بواسطة eSafety كجزء من مبادرة Be Connected.

eSafety Commissioner

Australian Government