Be Connected
Every Australian online.

Australian Government

مُلخّص العرض التقديمي عبر الإنترنت

هل يمكنك اكتشاف عمليات الاحتيال؟

إن إحدى أهم الخطوات لتجنّب الوقوع ضحية لعمليات الاحتيال عبر الإنترنت هي القدرة على التعرّف عليها وعلى كيفية عملها. يفقد الأستراليون المسنّون ملايين الدولارات كل عام بسبب عمليات الاحتيال. في حين أن الإنترنت هو مكان رائع للاستكشاف والتواصل مع الآخرين، غير أننا لا يمكننا دائماً التأكد من أن الأشخاص هم حقاً من يدّعون. بمجرد معرفة حيل المحتال، ستتمكن على الأغلب من التعرّف على عملية الاحتيال.

عمليات التصيّد الاحتيالية

عمليات التصيّد الاحتيالية هي عبارة عن محاولات يقوم بها المحتالون لخداعك وجعلك تصدّق بأنهم ينتمون لمنظمة موثوقة أو بأنهم شخصاً تعرفه، وذلك لكي تعطيهم تفاصيلك الشخصية كأرقام حسابك المصرفي وكلمات المرور وأرقام بطاقة الائتمان.

يتمّ تصميم رسائل التصيّد الاحتيالية لتبدو حقيقية وغالباً ما تنسخ التنسيق المُستخدم من قبل المنظمة التي يتظاهر المحتال بتمثيلها بما في ذلك علامتها التجارية وشعارها. قد تتّخذ عمليات الاحتيال هذه أشكالاً عديدة كرسائل البريد الإلكتروني أو الرسائل إلى هاتفك أو مكالمات هاتفية. على سبيل المثال، قد تصلك:

- رسالة إلى هاتفك تدّعي أنها من البنك الذي تتعامل معه وتطلب منك تأكيد كلمة المرور الخاصة بك
- رسالة إلى بريدك الإلكتروني تدّعي أنها من شركة الإنترنت وتطلب منك تحديث تفاصيلك
- رسالة إلى هاتفك تدّعي انها من أحد أفراد عائلتك وهو يستخدم رقم هاتف جديد، يخبرك أنه فقد هاتفه ويطلب منك إرسال الأموال على وجه السرعة
- مكالمة هاتفية من المؤسسة المالية التي تتعامل معها تنبّهك إلى "نشاط غير مُصرّح به أو مُريب على حسابك" أو أنه سيُغلق حسابك إذا لم تحدّث تفاصيلك
- إشعار من Facebook من شخص تعرفه يوصيك بتصفح موقع إلكتروني.

عمليات الاحتيال من خلال الضرائب و Medicare

ينتحل المحتالون صفة موظفي مكتب الضرائب الأسترالي (ATO) وMedicare والمؤسسات الحكومية الأخرى من أجل محاولة خداعك لدفع الأموال وإعطائهم معلوماتك الشخصية. يصمّم هؤلاء المحتالون مواقع إلكترونية مُزيّفة ويرسلون إليك رسائل عبر البريد الإلكتروني ورسائل إلى هاتفك ويتصلون بك هاتفياً متظاهرين أنهم من منظمة حكومية.

لن يرسل مكتب الضرائب أبداً رسالة عبر البريد الإلكتروني أو رسالة إلى هاتفك ولن يتصل بك هاتفياً ويطلب منك ما يلي:

- تقديم معلومات شخصية كرقم الملف الضريبي أو رقم بطاقة الائتمان أو تفاصيل حسابك المصرفي
- دفع رسوم لتلقي العائد الضريبي، أو دفع الأموال لكي لا يتمّ إلقاء القبض عليك بتهمة التهرّب من دفع الضرائب
- النقر على رابط لإدخال تفاصيلك الشخصية
- تنزيل الملفات أو تثبيت برنامج.

إن لم تكن متأكداً من أن الرسالة واردة من مكتب ATO، يمكنك الاتصال بالخط الساخن 1800 008 540 أو زيارة الموقع الإلكتروني ato.gov.au/scams.

كيف تحمي نفسك

- خذ وقتك. اقرأ الرسالة مرة أخرى. اسأل نفسك هل يمكن أن تكون الرسالة أو المكالمة مُزيّفة؟
- هل هو عنوان بريد إلكتروني رسمي أم يبدو وكأن فيه أخطاء؟
- إلى من تم توجيهها؟ إذا كانت موجّهة إلى "عزيزي الزبون" بدلاً من اسمك فينبغي عليك أن تشك في صحتها.
- هل تحتوي على أخطاء إملائية أو نحوية؟ يمكن أن يكون هذا علامة على أنها واردة من مُخادع.
- لا تستخدم تفاصيل الاتصال الواردة في الرسالة فهي قد تكون مُزيّفة. ابحث على الإنترنت عن رقم هاتف المنظمة وموقعها الإلكتروني الرسمي.
- لا تنقر على أي روابط أو تفتح أي مُرفقات لأنها قد تُنزِل فيروساً على جهازك - ما عليك إلا حذفها.
- لا تعطِ تفاصيل شخصية كرقم ملفك الضريبي (TFN) أو تاريخ ميلادك أو تفاصيل حسابك المصرفي أو تفاصيل بطاقة الائتمان.

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.

عمليات الاحتيال الرومانسية والصداقات

يستغل المحتالون الأشخاص الذين يبحثون عن أصدقاء أو شركاء رومانسيين، غالباً عبر مواقع المواعدة أو التطبيقات أو وسائل التواصل الاجتماعي أو حتى الألعاب عبر الإنترنت من خلال التظاهر بأنهم رفقاء مُحتملين. وهدفهم هو كسب ثقتك للحصول على الأموال أو الهدايا أو الصور الحميمة أو التفاصيل الشخصية.

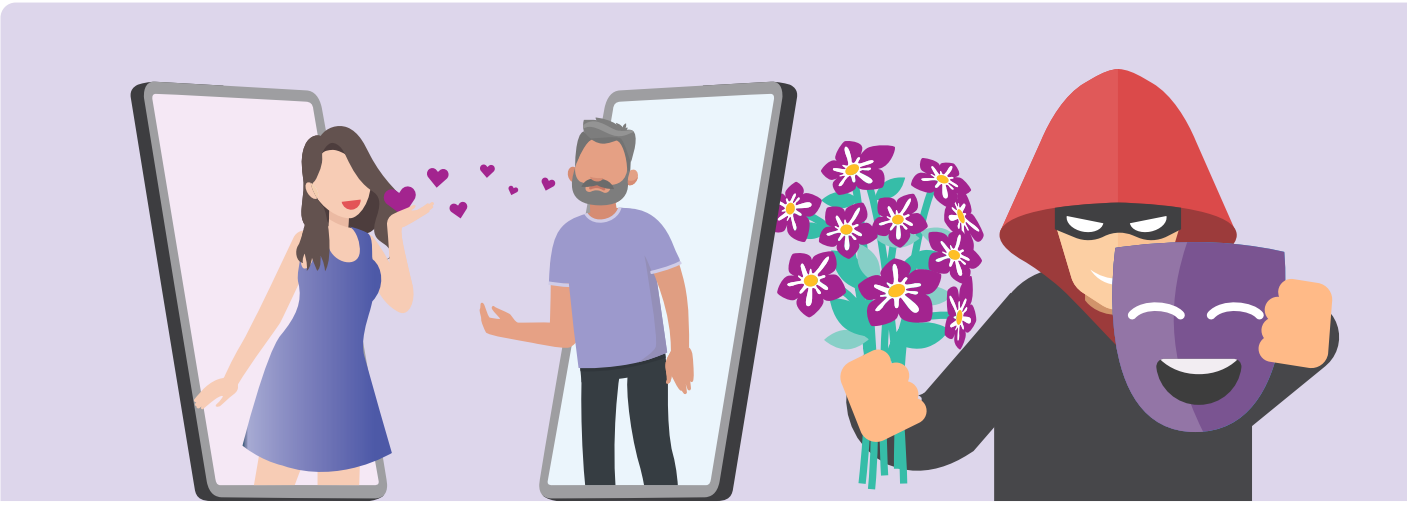
ما الذي يمكنك فعله لكي تكون واعياً وآمناً؟

تنبّه للشخص الذين يقوم بما يلي:

- يعترف بحبّه العميق لك بسرعة
- بعد اكتساب ثقتك - غالباً ما يأخذ وقته وينتظر أسابيع أو أشهر أو حتى سنوات - سيخبرك بقصة مُفصّلة ويطلب منك إرسال الأموال أو إقراضها له أو إرسال الهدايا أو إعطائه تفاصيل حسابك المصرفي/بطاقة الائتمان
- يتجنّب الالتقاء بك شخصياً ويختلق الأعذار لعدم تمكّنه من السفر لمقابلتك
- لديه ملف تعريف على الإنترنت لا يتوافق مع ما يُخبرك به عن نفسه.

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 في صور Google عن صور الشخص للمساعدة في تحديد ما إذا كان هو بالفعل من يدّعيه أو لمعرفة ما إذا كانت الصور قد تم أخذها من مكان آخر على الإنترنت. 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 وقواعد اللغة السيئة والتناقضات في القصص.
- لا تشارك الصور أو مقاطع الفيديو الحميمة. من المعروف أن المحتالين يبتزون ضحيتهم باستخدام مواد فاضحة.



حيل الدعم التقني

تبدأ عمليات الاحتيال هذه عادةً بمكالمة هاتفية أو بريد إلكتروني يبدو أنه من شركة اتصالات أو كمبيوتر كبيرة مثل Telstra و NBN و Microsoft لإخبارك أن لديك مشكلة في الكمبيوتر أو الإنترنت ويمكنهم إصلاحها. سيطلبون بعد ذلك الوصول عن بُعد إلى جهاز الكمبيوتر "لمعرفة المشكلة" أو يحاولون إقناعك بشراء برامج أو خدمة غير ضرورية "لإصلاح" الكمبيوتر.

كيف تحمي نفسك

- إذا تلقيت مكالمة هاتفية غير متوقّعة حول جهاز الكمبيوتر وطُلِب منك الوصول عن بُعد إلى جهاز الكومبيوتر - اقفل الخط.
- لا تسمح لمكالمة غير متوقّعة بالوصول عن بعد إلى جهاز الكمبيوتر.
- لا تشارك معلوماتك الشخصية كحسابك المصرفي أو تفاصيل بطاقة الائتمان.
- لا تشتري برامج من مكالمة هاتفية أو بريد إلكتروني غير متوقّع.
- تجاهل الرسائل المنبثقة التي تخبرك بالاتصال بالدعم التقني.

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. إذا لم تكن متأكداً، قل لهم لا واقفل الخط أو احذف الرسالة.

احم

- 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

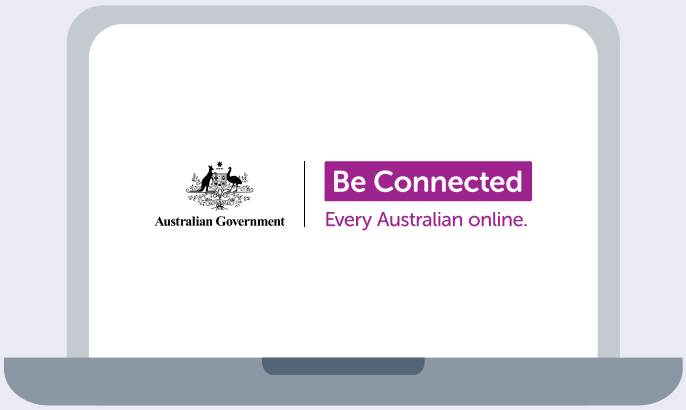
- اتصل بالبنك أو المؤسسة المالية التي تتعامل معها على الفور وأوقف أي دفعات إضافية إلى المحتال.
- إذا وقعت ضحية لجريمة عبر الإنترنت وخسرت أموالاً، فيمكنك إبلاغ الشرطة عن طريق ReportCyber أو زيارة الموقع الإلكتروني: cyber.gov.au
- إذا كنت قلقاً من أنه تمّ الكشف عن معلوماتك الشخصية وإساءة استخدامها، فاتصل 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