AUSTRALIAN COMPETITION & CONSUMER COMMISSION

الكُتيِّب الأسود حول الرسائل الاحتيالية

دليل بحجم الجيب لكي تتمكن من التعرُّف على الرسائل الاحتيالية وتجنبها وحماية نفسك منها

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

الكُتيِّب الأسود حول الرسائل الاحتيالية

دليل بحجم الجيب لكي تتمكن من التعرُّف على الرسائل الاحتيالية وتجنبها وحماية نفسك منها

ISBN 978 1 920702 00 7

المفوضية الأسترالية للمنافسة المستهلك (Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

يجب إرسال الطلبات والاستفسارات المتعلقة بالنسخ والحقوق إلى:
Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601,
أو publishing.unit@accc.gov.au.

ACCC 12/16_1129

www.accc.gov.au

المحتويات

مقدمة

في كل عام، تكلف الرسائل الاحتيالية الأستراليين والشركات والاقتصاد مئات الملايين من الدولارات وتتسبب في أذى عاطفي للضحايا وعائلاتهم.

أفضل طريقة لحماية نفسك هي من خلال الوعي والتعليم. هذه النسخة الجديدة من كتيِّب The *Little Black Book of Scams* *(الكُتيِّب الأسود حول الرسائل الاحتيالية)* مقدمة إليك من قبل المفوضية الأسترالية للمنافسة وحماية المستهلك (ACCC)، وهي الوكالة الوطنية لحماية المستهلك. إنّ الكُتيِّب الأسود حول الرسائل الاحتيالية مُعترفٌ به دولياً كأداة مهمة للمستهلكين والشركات الصغيرة للتعرُّف على الرسائل الاحتيالية بما في ذلك:

- الرسائل الاحتيالية الأكثر شيوعاً للانتباه لها
- الطرق المختلفة التي يستطيع بها المحتالون التواصل معك
- الأدوات التي يستخدمها المحتالون لخداعك
- علامات التحذير
- كيف تحمي نفسك، و
- أين يمكنك العثور على المساعدة.

الكُتيِّب الأسود حول الرسائل الاحتيالية متاح عبر الموقع الإلكتروني www.accc.gov.au/littleblackbookofscams.

حماية نفسك - اشترك في Scamwatch

للتفوق على المحتالين، تعرَّف على المزيد من خلال زيارة موقع Scamwatch الإلكتروني www.scamwatch.gov.au التابع لـ ACCC حيث يمكنك التسجيل للحصول على تحذيرات مجانية بالبريد الإلكتروني بشأن الرسائل الاحتيالية الجديدة التي تستهدف المستهلكين والشركات الصغيرة. ويمكنك أيضاً متابعة Scamwatch على تويتر عبر @scamwatch_gov أو http://twitter.com/scamwatch_gov.

أكثر رسائل احتيالية يجب تجنبها

الجميع عُرضة للرسائل الاحتيالية لذلك كل فرد بحاجة إلى معلومات حول كيفية التعرُّف على الرسائل الاحتيالية وتجنبها. يعتقد بعض الناس أن السُذج والجشعين فقط يقعون ضحية للرسائل الاحتيالية. الحقيقة هي أن المحتالين أذكياء وإذا كنت لا تعرف ما يجب أن تحترس منه، يمكن لأي شخص أن يقع ضحية للاحتيال.

هل تلقيت عرضاً يبدو جيداً بدرجة لا يمكن تصديقها، وربما مكالمة هاتفية للمساعدة في إصلاح جهاز الكمبيوتر الخاص بك أو تهديد بضرورة سداد أموال لا يجب عليك دفعها، أو تنبيه من البنك أو مقدم خدمة الاتصالات عن مشكلة في حسابك أو حتى دعوة لك "للصداقة" أو للتواصل عبر الإنترنت؟ المحتالون يعرفون كيف يضغطون عليك للحصول على ما يريدون.

إنهم يزدادون ذكاءاً ويستفيدون مع الوقت من أية تقنية أو منتجات أو خدمات جديدة وأحداث كبرى لتأليف قصص يمكن تصديقها لاقناعك بإعطاء أموالك أو بياناتك الشخصية.

ومع ذلك، واستناداً إلى عشرات الآلاف من التقارير المتعلقة بالرسائل الاحتيالية المستلمة كل عام، أعدّت ACCC قائمة بالرسائل الاحتيالية الشائعة للكشف عن الأسرار والتكتيكات التي لا يريدك المحتالون أن تعرفها.

الرسائل الاحتيالية للمواعَدة والعلاقات الرومانسية

تكلف الرسائل الاحتيالية للمواعَدة والعلاقات الرومانسية الأستراليين ملايين من الدولارات كل عام، ويمكن أن تدمر الأفراد والأسر.

كيفية عمل الرسالة الاحتيالية

يقوم المحتالون على سبيل **المواعَدة والعلاقات الرومانسية** بإنشاء حسابات مزيفة على مواقع التعارف الرسمية وتطبيقات الهواتف الذكية أو وسائل التواصل الاجتماعي مثل Facebook باستخدام صور وهويات غالباً ما تكون مسروقة من أشخاص آخرين، ويستخدمون هذه الحسابات الشخصية لمحاولة الدخول في علاقة معك يمكن أن تستمر لأشهر أو حتى سنوات، وذلك فقط لكي يتمكنوا من الاستيلاء على أموالك. وسيطلب المخادع مبالغاً مالية للمساعدة في مرض أو إصابة أو تكاليف سفر أو أزمة عائلية. المحتالون ليست لديهم شفقة وسوف يكذبون عليك للاستفادة من طبيعتك الأفضل.

عادةً ما يكون المحتالون خارج الدولة ولديهم سبب لتواجدهم هناك، مثل الخدمة العسكرية أو العمل كمهندس أو رعاية صديق أو قريب. إنهم ليسوا أبداً كما يقولون، وقد يرسل بعض المحتالين الأذكياء هدايا صغيرة. هذا ليس سوى جزء من خطتهم الكُبرى للحصول على المزيد من المال منك لاحقاً.

حماية نفسك

- لا ترسل أبداً أموالاً أو تقدم بياناتك الشخصية إلى شخص قابلته عبر الإنترنت فقط.
- راقب ما إذا كان أحد المعجبين عبر الإنترنت يطلب التواصل معك خارج موقع المواعَدة أو وسيلة التواصل الاجتماعي بعد عدد قليل من "مرات التواصل" أو المحادثات بينك ,والشخص - فقد يكون هذا الشخص مُحتالاً.
- ابحث بالصورة عن الشخص المُعجب لكي تعرف ما إذا كان حقاً كما يقول. ويمكنك استخدام خدمات البحث بالصورة مثل Google أو TinEye.
- كُن حذراً عند مشاركة صور أو مقاطع فيديو حميمة عبر الإنترنت، فمن المعروف أن المحتالين يقومون بابتزاز ضحاياهم باستخدام صور أو مقاطع فيديو لك لا تريد أن يراها أحد.

رسائل الاستثمار الاحتيالية

"استثمار خالي من المخاطر" أم فرصة لسوء الحظ؟

كيفية عمل الرسالة الاحتيالية

تأتي **رسائل الاستثمار الاحتيالية** في أشكال عديدة، بما في ذلك شراء العملة المشفرة، وتجارة الخيارات الثنائية، والمشاريع التجارية، وبرامج الإدخار التقاعدي، والأموال المُدارة، وبيع أو شراء الأسهم أو العقارات. ويقوم المحتالون بعرض "الفرص" من خلال مطبوعات ذات مظهر احترافي ومواقع إلكترونية لإخفاء عملياتهم الاحتيالية. غالباً ما يبدأون بمكالمة هاتفية أو برسالة بريد إلكتروني غير متوقعة من الشخص المحتال يعرض فيها فرصة "لا ينبغي تفويتها" أو "ذات عائد مرتفع" أو "مضمونة". وعادةً ما يعمل المحتال من خارج الدولة، ولن تكون لديه رخصة أسترالية للخدمات المالية.

تعِد **الرسائل الاحتيالية من خلال برامج التنبؤ بالكمبيوتر** بالتنبؤ الدقيق بحركات سوق الأوراق المالية أو نتائج سباقات الخيل أو الأحداث الرياضية أو اليانصيب. إنها ببساطة شكل من أشكال المقامرة المقنعة كاستثمارات. وتكون معظم المشاريع أو البرامج وهمية ولا يمكن للمشترين استرداد أموالهم. في كثير من الحالات، يختفي مقدم العرض بكل بساطة.

تقدِّم **الرسائل الاحتيالية المتعلقة بالإدخار التقاعدي** عرضاً لمنحك إمكانية الوصول المبكر إلى مبالغ الإدخار التقاعدي الخاص بك، وغالباً من خلال صندوق إدخار تقاعدي مُدار ذاتياً أو مقابل رسم. وقد يطلب منك المحتال الموافقة على تأليف قصة للسماح بالإفراج المبكر عن أموالك، ومن ثمَّ، بصفته مستشاراً مالياً لك، فسوف يحتال على شركة الإدخار التقاعدي التي تتعامل معها لكي تدفع إليه مبشارةً مزايا إدخارك التقاعدي. وبمجرد حصوله على أموالك، قد يأخذ المحتال "رسوماً" كبيرة أو يتركك خالي الوفاض.

حماية نفسك

- لا تدع أي شخص يضغط عليك لاتخاذ قرارات بشأن أموالك أو استثماراتك - خاصة إذا كان العرض غير متوقعاً.
- قبل الإفراج عن أموالك، ابحث عن معلومات عن شركة الاستثمار وتحقق منها عبر www.moneysmart.gov.au لمعرفة ما إذا كان لديهم رخصة أسترالية للخدمات المالية. اسأل نفسك: إذا كان شخص غريب قد عرف سراً لكسب المال، فلماذا يتشارك فيه؟

إذا كنت أصغر من سن التقاعد، احترس من العروض التي تروِّج لسهولة الوصول إلى مزايا ادخارك التقاعدي. وإذا حصلت على ادخارك التقاعدي مبكراً بشكل غير قانوني، فقد تواجه عقوبات بموجب قانون الضرائب.

رسائل التهديد والعقوبات الاحتيالية

إذا طلبت منك هيئة حكومية أو شركة موثوق بها دفع أية مبالغ، توقف وفكر وتأكد من ذلك ..

كيفية عمل الرسالة الاحتيالية

بدلاً من تقديم جائزة أو مبالغ مالية أو خصومات، تأتيك هذه الرسائل الاحتيالية في شكل تهديدات مصمّمة لتخويفك لكي تدفع مبالغاً مالية. وقد يتواصل معك المحتال ويهددك **بالقبض عليك** أو يرسل لك رسالة بريد إلكتروني يدعي فيها أنه يجب عليك سداد قيمة غرامة مالية بسبب **مخالفة سرعة القيادة** أو **مبلغ أنت مَدين به لمكتب الضرائب** أو **فاتورة غير مدفوعة**.

أثناء المكالمة الهاتفية، سوف يقوم المحتالون بالضغط عليك للدفع على الفور وإخبارك بأنه سيتم إرسال الشرطة إلى منزلك إذا رفضت. ومن المعروف أن المحتالين يستهدفون الأشخاص المستضعفين في مجتمعنا، مثل المهاجرين الجُدد، ويدّعون أنهم موظفون في دائرة الهجرة ويهددون الضحايا **بالترحيل** ما لم يتم دفع رسوم لتصحيح أخطاء في تأشيراتهم. ويدّعي المحتال، ضمن عملية احتيال مشابهة للغاية، أنه من مكتب الضرائب الأسترالي ويخبر ضحاياه بأن لديهم فاتورة ضريبية يجب سدادها.

يتظاهر المحتالون أيضاً بأنهم **شركات موثوق بها** مثل البنك الذي تتعامل معه أو شركة الغاز أو الكهرباء أو الماء أو مقدم خدمة هاتفية. وسيهددون بإلغاء خدمتك أو فرض رسوم جزائية مفرطة إذا لم تدفع الفاتورة على الفور. وفي بعض الأحيان، قد ينتحلون شخصية شركة مثل Australia Post ويقولون لك أن لديك إرسالية يجب أن تستلمها أو سيتم محاسبتك على كل يوم لا تدفعه. ومهما كان الأمر، فهم يحاولون إثارة قلقك والتصرف بدون تفكير والتحقق من صحة القصة.

إذا تلقيت رسالة احتيالية بالبريد الإلكتروني، فمن المحتمل أن تتضمن مرفقاً أو رابطاً يؤدي إلى موقع إلكتروني مزيف حيث سيُطلب منك تنزيل إثبات "الفاتورة" أو "الغرامة" أو "تفاصيل التسليم". سيؤدي فتح المرفق أو تنزيل الملف إلى إصابة جهاز الكمبيوتر الخاص بك ببرامج ضارّة (راجع صفحة 16).

حماية نفسك

- لا تسمح بالضغط عليك من قبل المتصل الذي يهددك. توقف وفكر وتحقق مما إذا كانت قصته صحيحة.
- لن تطلب منك أية وكالة حكومية أو شركة موثوق بها أن تقوم بالدفع بطرق غير معتادة مثل بطاقة الهدايا أو التحويلات البنكية أو Bitcoins.
- تحقق من هوية المتصل عن طريق الاتصال بالمنظمة ذات الصلة مباشرةً - يمكنك العثور عليها من خلال مصدر مستقل مثل دفتر الهاتف أو الفاتورة السابقة أو البحث عبر الإنترنت.
- لا تستخدم تفاصيل الاتصال الواردة في رسائل البريد الإلكتروني أو المقدمة لك أثناء المكالمات الهاتفية. مرة أخرى، ابحث عنهم من خلال مصدر مستقل.

الرسائل الاحتيالية المالية غير المتوقعة

إذا طُلب منك دفع مبالغ مالية قبل استلام سلع أو أموال، فكر ملياً.

كيفية عمل الرسالة الاحتيالية

يخبرك المحتالون بشكل غير متوقع عن حقك في الحصول على مال أو أحجار كريمة ثمينة أو ذهب أو أسهم قيِّمة، لكن يتعين عليك دفع **مبالغ مقدماً** للحصول عليها. ولن تتلقى أبداً ما وعدوك به، بل سيكون هناك دائماً عذر لماذا يتعين عليك دفع المزيد. وإذا دفعت الرسوم، فسوف تخسر أموالك.

يخبرك المحتالون عبر **الرسائل الاحتالية المتعلقة بالخصم أو الاسترداد** بأنك مستحقاً لمبالغ مالية بسبب الضرائب الزائدة أو الرسوم المصرفية أو نوع من التعويض. ومع ذلك، قبل أن تحصل على أموالك، يُطلب منك دفع رسوم إدارية صغيرة.

في **الرسائل الاحتالية المتعلقة بالميراث**، ينتحل المحتالون شخصية محامين أو مصرفيين أو مسؤولين أجانب ويخبرونك بأنه يحق لك الحصول على ميراث كبير أو يعرضون عليك حصة في مشروع لأنك تحمل نفس اسم شخص توفي. وغالباً ما يستخدمون مستندات ذات مظهر رسمي ويطلبون منك سداد رسوم وضرائب قبل أن تتمكن من الحصول على الميراث. ويمكن أيضاً أن يطلبوا بياناتك الشخصية لإكمال "أوراق رسمية". هذا يعني أنه قد تكون تمت سرقة هويتك وأموالك أيضاً.

قد تكون الرسائل الاحتيالية المعروفة شيوعاً باسم **الرسائل الاحتيالية النيجيرية** قد نشأت في غرب إفريقيا ولكنها يمكن أن تأتي من أي مكان في العالم. وفي هذه الرسائل، يخبرك المحتالون بأنهم بحاجة لمساعدتك لتأمين ثروة كبيرة يحاولون جاهدين نقلها إلى خارج بلدهم. وقد يزعمون أن الثروة عبارة عن مال أو ذهب أو أصول مخبأة تخلت عنها حكومة أو مسؤول فاسد، وإذا وافقت على استلامها، فسوف يعطونك حصة كبيرة عندما يكون ذلك

آمناً. مثل كافة الرسائل الاحتيالية من هذا النوع، سيقولون إن عليك أولاً دفع ضرائب أو رسوم مصرفية أو رسوم مكافحة الإرهاب ورسوم التحقق من عمليات غسيل الأموال قبل أن يتمكنوا من إرسال الأموال.

عادةً ما تأتي هذه الرسائل الاحتيالية من الخارج وتطلب الدفع عن طريق حوالة برقية، ولكنها قد تطلب أيضاً تحويلات بنكية أو طرق دفع أخرى.

إذا وقعت ضحية لهذه الرسائل الاحتيالية، فلن تتلقى أبدًا أي شيء من الشخص المحتال وستفقد أية مبالغ مالية أرسلتها.

حماية نفسك

- تذكر أنه لا توجد مشاريع للثراء السريع: إذا بدا الأمر جيداً للغاية بحيث يصعب تصديقه، فمن المحتمل أن يكون عملية احتيال.
- تجنب أي ترتيب مع شخص غريب يطلب الدفع مقدماً عبر حوالة بريدية أو حوالة برقية أو حوالة مالية دولية أو بطاقة مسبقة التغذية أو عملة إلكترونية. ومن النادر استعادة الأموال المرسلة بهذه الطريقة.
- إذا ساورك الشك بشأن رسالة بريد إلكتروني غير مرغوب فيها، فامسحها. لا تنقر على أية روابط.
- لن تتواصل معك الدوائر الحكومية أو البنوك أو شركات الخدمات الاستهلاكية لكي تطلب منك دفع مبالغ مقدمة للمطالبة برسم أو خصم.
- إذا كنت غير متأكد، تحقق من هوية المتصل بشكل مستقل. ولا تستخدم تفاصيل الاتصال الواردة في الرسالة المرسلة إليك - احصل على تفاصيل الاتصال الصحيحة من خلال مصدر مستقل مثل دفتر الهاتف أو البحث عبر الإنترنت.
- قم بالبحث على الإنترنت باستخدام نفس صيغة العرض بشكل دقيق - يمكن التعرُّف على العديد من الرسائل الاحتيالية بهذه الطريقة.

رسائل الجوائز واليانصيب الاحتيالية

لا يغويك الفوز المفاجئ - المحتال فقط هو الذي يحصل على مكاسب مفاجئة.

كيفية عمل الرسالة الاحتيالية

تحاول هذه الرسائل الاحتيالية خداعك لدفع مبالغ مالية مقدماً أو إعطاء بياناتك الشخصية للحصول على جائزة من اليانصيب أو رهان أو منافسة لم تدخلها مطلقاً. ويزعم المحتالون أنه يتعين عليك دفع رسوم أو ضرائب قبل الإفراج عمّا "ربحته" أو جائزتك. وقد تضطر أيضاً إلى الاتصال أو إرسال رسالة نصية إلى رقم هاتف ذي سعر عالي للمطالبة بجائزتك.

وفي **رسائل بطاقات الكشط الاحتيالية**، يأتيك بريد يحتوي على كتيبات لامعة وعدد من بطاقات الكشط، بحيث ستكون إحداها هي الفائزة. ولجعل الأمر أكثر تصديقاً، ستكون غالباً الجائزة الثانية أو الثالثة. وعند الاتصال للمطالبة بجائزتك، سيطلب المحتالون دفع رسوم أو ضرائب قبل أن تتمكن من الحصول على ما ربحته.

قد تستخدم **رسائل اليانصيب الاحتيالية** أسماء يانصيب حقيقية خارج الدولة لإخبارك بأنك ربحت أموالاً، على الرغم من أنك لم تدخل اليانصيب على الإطلاق. و عادةً ما يطلب المحتالون رسوماً أو ضرائب للإفراج عن الأموال. وسيخبرونك أيضاً بأنهم يحتاجون بياناتك الشخصية لإثبات أنك الفائز الصحيح ولكن بعد ذلك يستخدمون هذه المعلومات لسرقة هويتك أو مالك من حسابك المصرفي.

في عمليات الاحتيال **بالقسائم وبطاقات الهدايا المزيفة**، يرسل المحتالون إليك رسالة بريد إلكتروني أو رسالة نصية أو رسالة عبر وسائل التواصل الاجتماعي يخبرونك فيها بأنك فزت ببطاقة هدايا لدى أحد متاجر التجزئة المعروفة ولكن يتعين عليك تقديم بعض التفاصيل قبل أن تتمكن من المطالبة بها. وهذه محاولة للحصول على معلومات شخصية يمكن استخدامها لسرقة الهوية أو لاستهدافك باحتيال آخر. وهناك عروض مثل هذه معروفة أيضاً لكي يُطلب منك تقديم فدية على جهازك (راجع صفحة 17).

في **عمليات الاحتيال بجائزة سفر**، يخبرك المحتالون بأنك ربحت عطلة مجانية أو تذاكر طيران. في الواقع، إنّ ما فزت به فعلاً هو فرصة شراء قسائم سكن أو طيران. وغالباً ما يكون لقسائم السفر هذه رسوم وشروط مخفية، أو قد تكون وهمية ولا قيمة لها. وبالمثل، قد يقدم لك المحتالون باقات عطلات رائعة بأسعار مخفضة لا وجود لها.

حماية نفسك

- تذكَّر: لا يمكنك كسب المال في اليانصيب أو المسابقة ما لم تكن أصلاً دخلت فيها.
- لا تتطلب منك المسابقات واليانصيب دفع رسوم لاستلام ما ربحته - ابحث عبر الإنترنت باستخدام نفس صيغة العرض بشكل دقيق. وقد يساعد ذلك في التأكيد على أنها عملية احتيالية.
- فكر ملياً قبل الاتصال أو إرسال رسائل نصية برقم هاتف يبدأ بـ "19" – تُفرض عليها رسوم عالية.

التسوق الإلكتروني، الإعلانات المبوّبة والمزادات الاحتيالية

المحتالون يحبون التسوق الإلكتروني السهل أيضاً.

كيفية عمل الرسالة الاحتيالية

يقوم المستهلكون والشركات بعمليات بيع وشراء إلكتروني بشكلٍ متزايد. وللأسف، يحب المحتالون البحث عن ضحايا عبر الإنترنت.

يستطيع المحتالون إنشاء **مواقع إلكترونية مزيفة ومقنعة لمتاجر تجزئة** تبدو كأنها حقيقية، بما في ذلك على وسائل التواصل الاجتماعي مثل Facebook. أكبر دليل على أن موقع التجزئة احتيالي هي طريقة الدفع - كن حذراً إذا طلب منك الدفع عن طريق التحويل البنكي أو غيره من الطرق غير المعتادة.

في **عمليات الاحتيال بالمزاد الإلكتروني**، يدّعي المحتال أن لديك فرصة ثانية لشراء شيء زايدتَ عليه لأن الفائز قد انسحب. وسيطلب منك المحتال الدفع خارج وسيلة الدفع الآمنة لموقع المزاد؛ إذا قمت بذلك، فستضيع أموالك ولن تحصل على ما دفعته ولن يتمكن موقع المزاد من مساعدتك.

الاحتيال بالإعلانات الإلكترونية المبوبة هو عملية احتيال شائعة تستهدف كل من المشترين والبائعين. ويجب على المشترين الحذر من المحتالين الذين يقومون بنشر إعلانات وهمية على مواقع الإعلانات المبوبة المشروعة. ويمكن أن تكون الإعلانات لأي شيء بدءاً من تأجير العقارات إلى الحيوانات الأليفة أو السيارات أو الكاميرات المستعملة، وغالباً ما يتم تسعيرها بأسعار رخيصة. وإذا أبديت اهتماماً بشيءٍ ما، فقد يدعي المحتال أنه مسافر أو قد

انتقل إلى الخارج وأن الوكيل سوف يقوم بتسليم البضاعة بعد استلام المبلغ. وبعد الدفع، لن تتلقى السلع ولن تستطيع الاتصال بالبائع.

بالنسبة للبائعين، سوف يتقدَّم محتال الاعلان المبوب بعرض سخي لإعلانك. وإذا قبلت ذلك، فسيدفع المحتال بموجب شيك أو حوالة بريدية. ومع ذلك، فإن المبلغ الذي تتلقاه يكون أكثر من السعر المتفق عليه. في عملية **الاحتيال بالدفع الزائد** هذه، قد يخبرك "المشتري" أن هذا كان خطأ وسيطلب منك ردّ المبلغ الزائد عن طريق حوالة مالية. ويأمل المحتال في أن تقوم بتحويل المبلغ قبل أن تكتشف أن شيكه قد ارتد أو أن الحوالة البريدية كانت مزيفة. وسوف تخسر المال، وكذلك الشيء الذي قمت ببيعه إذا كنت قد أرسلته بالفعل.

حماية نفسك

- اعرف بالضبط مع من تتعامل. وإذا كان تاجر تجزئة أسترالي، فأنت في وضع أفضل بكثير لحل المشكلة إذا حدث خطأ ما.
- تحقق مما إذا كان البائع يتمتع بسمعة طيبة ولديه سياسة للمبالغ المستردة وخدمات للتعامل مع الشكاوى.
- تجنب أي ترتيب يطلب الدفع مقدماً عبر حوالة بريدية أو حوالة بنكية أو حوالة مالية دولية أو بطاقة مسبقة التغذية أو عملة إلكترونية. من النادر استعادة الأموال المرسلة بهذه الطريقة. ولا ترسل أبداً أموالاً أو تقدم تفاصيل بطاقة إئتمانية أو حساب إلكتروني لأي شخص لا تعرفه ولا تثق فيه، ولا يكون ذلك أبداً عبر البريد الإلكتروني.
- ادفع فقط من خلال طريقة الدفع الإلكتروني الآمنة - ابحث عن عنوان موقع إلكتروني يبدأ بـ 'https' ويحتوي على رمز قفل مغلق.
- لا تقبل أبداً شيكاً أو حوالة بريدية بدفع أكثر مما اتفقت عليه ولا ترسل مالاً لأي شخص.

الرسائل الاحتيالية التي تستهدف أجهزة الكمبيوتر والأجهزة المحمولة

تذكر: أي شيء يتصل بالإنترنت عُرضة للخطر.

كيفية عمل الرسالة الاحتيالية

يقوم **المحتالون الذين يستخدمون تقنيات الوصول عن بُعد** بالاتصال بك عبر الهاتف مدعين أن جهاز الكمبيوتر الخاص بك مُصاب بفيروسات. وإذا اتبعت الإرشادات الخاصة بهم، فستسمح لهم بالوصول إلى جهاز الكمبيوتر الخاص بك والتحكم فيه حيث يمكنهم سرقة المعلومات أو تركيب برامج ضارة. وقد يحاولون أيضاً إقناعك بشراء برنامج "مكافحة الفيروسات"، والتي عادةً ما تكون أسعارها باهظة أو قد تكون متاحة مجانًا على الإنترنت.

البرامج الضارة هي مصطلح لأي برامج حاسوبية ضارة يمكن تركيبها على جهاز الكمبيوتر الخاص بك أو غيره من الأجهزة، بما في ذلك الفيروسات وبرامج التجسس وبرامج الفدية وأحصنة طروادة وبرامج رصد لوحة المفاتيح.

تسمح **برامج رصد لوحة المفاتيح وبرامج التجسس** للمحتالين بتسجيل ما تكتبه بالضبط على لوحة المفاتيح للعثور على كلمات المرور والتفاصيل المصرفية أو الوصول إلى المعلومات الشخصية وإرسالها إلى أي مكان يريدونه. وبمجرد تركيب هذه البرامج، يستطيع المحتالون التحكم في بريدك الإلكتروني وحسابات التواصل الاجتماعي والحصول على أية معلومات موجودة على جهازك، بما في ذلك كلمات المرور. ويستطيعون أيضاً استخدام حساباتك لإرسال المزيد من الرسائل الاحتيالية إلى أصدقائك وعائلتك.

برنامج الفدية هو نوع آخر من البرامج الضارة التي تقوم بتشفير أو قفل جهازك لمنعك من استخدامه حتى يتم إجراء الدفع لفتحه أو فكّ شيفرته. ولا يضمن الدفع أنه سيتم فتح الجهاز أو إلغاء شيفرته أو خلوه من الفيروسات المخفية، والتي يمكنها أيضاً أن تنتشر وتصيب أجهزة الكمبيوتر أو الأجهزة الأخرى على شبكتك.

يتم تسليم البرامج الضارة بشكل شائع عبر البريد الإلكتروني، ويمكن أن تبدو أنها من مصادر مشروعة، مثل مقدم الخدمة أو وكالة حكومية أو حتى الشرطة وتدعي إصدار غرامة لك. لا تنقر على الرابط أو تفتح أية مرفقات لا تعرفها جيداً. ربما تقوم بتنزيل برامج ضارة بدلاً من ذلك. ويستهدف هذا النوع من الرسائل الاحتيالية كل من الأفراد والشركات.

حماية نفسك

- احترس من تنزيل المواد المجانية المحتوية على موسيقى وألعاب وأفلام والوصول إلى مواقع البالغين، فقد يقومون بتركيب برامج ضارة بدون علمك.
- حافظ على أمان شبكات مكتبك وأجهزة الكمبيوتر والأجهزة المحمولة الخاصة بك. قم بتحديث برنامج الأمان الخاص بك وتغيير كلمات المرور وعمل نسخة احتياطية من بياناتك بانتظام. قم بتخزين النسخ الاحتياطية الخاصة بك في ملفات خارجية وغير متصلة بالشبكة. يشرح الموقع الإلكتروني www.staysmartonline.gov.au كيفية عمل نسخة احتياطية من بياناتك وتأمين أجهزتك المحمولة.
- لا تفتح أية مرفقات أو تنقر على روابط في رسائل البريد الإلكتروني أو رسائل التواصل الاجتماعي التي تأتيك من أشخاص غرباء - فقط انقر على زر المسح.

سرقة الهوية

يُحتمل أن تتم في جميع الرسائل الاحتيالية سرقة الهوية. حماية نفسك من الرسائل الاحتيالية تعني أيضاً الحفاظ على أمان معلوماتك الشخصية.

تشكل سرقة الهوية تهديداً في كل رسالة احتيالية

يربط معظم الأشخاص بين الرسائل الاحتيالية ومحاولات الاستيلاء على أموالك. ومع ذلك، فإن معلوماتك مهمة أيضاً للمحتالين، حيث يقوم المحتالون بسرقة بياناتك الشخصية للقيام بأنشطة احتيالية مثل عمليات شراء غير مصرح بها ببطاقتك الائتمانية، أو استخدام هويتك لفتح حسابات بنكية أو هاتفية. وقد يحصلون على قروض أو يقومون بأعمال تجارية غير قانونية أخرى باسمك. كما قد يبيعون معلوماتك إلى محتالين آخرين للمزيد من الاستخدام المخالف للقانون.

إن سرقة هويتك يمكن أن تكون مدمرة مالياً وعاطفياً. وقد يستغرق الأمر عدة أشهر لاستعادة هويتك، وقد يستمر تأثير سرقتها لسنوات.

التصيُّد الاحتيالي - يتصل بك الشخص المحتال بشكل مفاجئ عبر البريد الإلكتروني أو الهاتف أو Facebook أو عبر رسالة نصية ويتظاهر بأنه يمثل عملاً تجارياً مشروعاً مثل بنك أو مقدم خدمات هاتف أو إنترنت. يوجهك المحتال إلى موقع إلكتروني مزيف خاص بالعمل التجاري ويطلب فيه بياناتك الشخصية للتحقق من سجلات العملاء بسبب خطأ فني. وقد يتصل مُدعياً أنه تاجر تجزئة لسلع فاخرة ويزعم أن شخصاً ما يحاول استخدام بطاقتك الائتمانية، وينصحك بالاتصال بالبنك الذي تتعامل معه ولكنه لا ينهي المكالمة من جانبه ويبقي على الخط مفتوحاً. وعند محاولة الاتصال بالبنك، لا تزال تتحدث إلى المحتال الذي يحاكي مكالمة حقيقية ويقلد موظف البنك ويطلب منك تفاصيل حسابك المصرفي وبياناتك الأمنية. في كلتا الحالتين، يلتقط المحتال أية معلومات تقدمها له، ثم يستخدمها للوصول إلى حساباتك.

الاستبيانات المُزيفة - يقدِّم المحتالون جوائزاً أو مكافآت مثل بطاقات الهدايا إلى تجار التجزئة المعروفين مقابل استكمال استبيان عبر الإنترنت. ويطلب منك الاستبيان الإجابة على مجموعة من الأسئلة بما في ذلك الكشف عن تفاصيل هوية مهمة أو بيانات مصرفية.

كجزءٍ من أية رسالة احتيالية - غالباً ما يطلب المحتالون معلومات شخصية في رسائل احتيالية أخرى. في رسائل اليانصيب الاحتيالية، يطلب المحتالون في كثير من الأحيان الحصول عن بيانات رخصة القيادة أو جواز السفر "لإثبات هويتك قبل أن يتمكنوا من الإفراج عن أموال الجائزة". وفي رسائل المواعَدة والعلاقات الرومانسية الاحتيالية، قد يطلبون معلومات "لكفالة طلب تأشيرتهم لزيارتك في أستراليا".

تذكر: إن إعطاء المعلومات الشخصية لأحد المحتالين قد يكون بنفس سوء إعطاء المال. حافظ على بياناتك الشخصية لنفسك واحتفظ بها آمنة.

حماية نفسك

- **فكر ملياً فيما تقوله وتفعله في أية بيئة عبر الإنترنت**

كن حذراً عند مشاركة أية معلومات عنك عبر الإنترنت، بما في ذلك وسائل التواصل الاجتماعي والمدونات والمنتديات الأخرى عبر الإنترنت. توقف وفكر قبل إكمال الاستبيانات أو الدخول في المسابقات أو النقر على الروابط أو المرفقات أو حتى "المصادقة" أو "الإعجاب" أو "مشاركة" شيءٍ ما عبر الإنترنت.

- **احذر من أي طلب للحصول على تفاصيلك أو مالك**

سيحاول المحتالون خداعك لتعطيهم بياناتك باستخدام أسماء شركات معروفة أو دوائر حكومية. إذا كنت تعتقد أنك تلقيت رسالة احتيالية، فلا ترد عليها. استخدم دفتر الهاتف أو ابحث عبر الإنترنت للتحقق من تفاصيل الاتصال بالمنظمة. لا تستخدم أبداً تفاصيل الاتصال الواردة في الطلب الأصلي.

إذا كنت قدَّمت معلومات هويتك الشخصية لمحتالين، اتصل بـ IDCARE على الرقم 1300 432 273.

الرسائل الاحتيالية المتعلقة بالعمل والتوظيف

دخل كبير ومضمون؟ هذا احتمال بعيد!

كيفية عمل الرسالة الاحتيالية

تتضمن **الرسائل الاحتيالية المتعلقة بالعمل والتوظيف** عروضاً للعمل من المنزل أو إنشاء والاستثمار في "فرصة عمل تجاري". يقدِّم المحتالون وعداً بوظيفة أو راتب عالي أو عائد استثماري كبير بعد دفعات مبدئية مقدَّمة. وقد تكون هذه المدفوعات مقابل "خطة عمل" أو دورة تدريبية أو برامج حاسوبي أو زي رسمي أو تصريح أمني أو ضرائب أو رسوم. وإذا دفعت الرسوم، فقد لا تتلقى أي شيء أو ما توقعته أو وعدوك به.

قد تكون بعض عروض العمل بمثابة غطاء **لأنشطة غسيل أموال غير مشروعة**، حيث يُطلب منك العمل "كمدير حسابات" أو "مساعد شخصي"، وتتلقى مدفوعات في حسابك المصرفي مقابل عمولة، ومن ثمَّ يتم نقل الأموال إلى شركة أجنبية.

وغالباً ما تأتي رسائل العمل الاحتيالية من خلال صندوق رسائل البريد الإلكتروني غير المرغوب فيها (spam email) أو عبر إعلانات في صفحة إعلانات مبوبة معروفة وعلى مواقع الباحثين عن عمل - حتى المواقع الحكومية للباحثين عن عمل.

يتمثل الخطر الكبير في هذا النوع من الرسائل الاحتيالية في أنه يمكن أن يطلب منك الكثير من التفاصيل الشخصية التي يجب أن لا تقدمها، بما في ذلك رقم ملفك الضريبي ونسخ عن جواز سفرك أو رخصة قيادتك. ويمكن استخدام هذه المعلومات لاحقاً لسرقة الهوية.

حماية نفسك

- احذر من العروض أو المشاريع التي تطالب بضمان الدخل أو تتطلب الدفع مقدماً.
- لا توافق أبدًا على تحويل الأموال لشخص آخر - فهذا غسيل أموال وهو مخالف للقانون.
- لا تقدم رقم رقم ملفك الضريبي أو رخصة قيادتك أو جواز سفرك عند تقديم طلب لوظيفة. قد يتعين عليك تقديم هذه المعلومات ولكن فقط بعد أن تبدأ العمل.

غسيل الأموال هو جريمة جنائية: لا توافق على تحويل الأموال لشخص غريب.

الرسائل الاحتيالية المتعلقة بالأغراض الخيرية والحالات الطبية

المحتالون ليست لديهم شفقة، ويمكن أن يزاولوا أعمالهم الاحتيالية أثناء أوقات الحاجة الشديدة.

كيفية عمل الرسالة الاحتيالية

يستفيد المحتالون من الأشخاص الذين يسعون لتقديم تبرعات خيرية أو إيجاد حل لمشكلة صحية.

في **العمليات الاحتيالية المتعلقة بالأغراض الخيرية**، يقوم المحتالون بجمع الأموال من خلال الإدعاء بأنهم يقومون بعمل من أجل قضية أو مؤسسة خيرية مشروعة أو مؤسسة وهمية قاموا بإنشائها. وغالباً ما يستغل المحتالون كارثة أو أزمة طبيعية حدثت مؤخراً وتمت تغطيتها في الأخبار.

تقوم هذه الرسائل الاحتيالية بتحويل التبرعات التي تشتد الحاجة إليها بعيداً عن الجمعيات الخيرية المشروعة. ويجب أن تكون المؤسسات الخيرية مسجلة لدى الحكومة - تبرع بثقة عن طريق التحقق من تسجيلها أولاً.

تعرض رسائل **العلاج المعجزة (Miracle cure)** مجموعة من المنتجات والخدمات التي يمكن أن تبدو أدوية بديلة مشروعة، عادةً ما تعد بعلاجات سريعة وفعالة للحالات الطبية الخطيرة. وغالباً ما يتم الترويج للعلاجات باستخدام إفادات مزيفة من أشخاص تمّ علاجهم.

تقدِّم **الرسائل الاحتيالية المتعلقة بفقدان الوزن** وعوداً بفقدان قدر كبير في الوزن مع بذل جهد ضئيل أو بدون مجهود. وقد يشتمل هذا النوع من الرسائل الاحتيالية على نظام غذائي غير عادي أو مقيد أو تمرين قاسي أو جهاز "للتخلص من الشحوم" أو حبوب منع الحمل أو لصاقات أو كريمات. وقد يُطلب منك سداد دفعة مقدمة كبيرة أو الدخول في عقد طويل الأجل لتلقي الإمدادات المستمرة.

تقدِّم **الصيدليات المزيفة عبر الإنترنت** عقاقيراً زائفة بأسعار رخيصة جداً، وأحياناً تقدمها بدون وصفة طبية. وقد تحتوي هذه الأدوية على مكونات نشطة محدودة أو لا تحتوي على مكونات فعالة، مما قد يؤدي إلى عواقب مهلكة للمستخدمين.

حماية نفسك

- إذا تمَّ الاتصال بك من قبل أحد جامعي التبرعات الخيرية في الشارع، فاطلب رؤية هويته. وإذا كانت لديك أية شكوك حول هويته، لا تتبرع له.
- راجع قائمة الجمعيات الخيرية الأسترالية غير الربحية لمعرفة الجمعيات الخيرية المسجلة.
- استشر أخصائي الرعاية الصحية إذا كنت تفكر في تقديم مطالبة علاج "معجزة" أو "فوري" بشأن أدوية أو مكملات غذائية أو غيرها من العلاجات.
- اسأل نفسك: إذا كان هذا علاجاً معجزة حقًّا، أما كان أخصائي الرعاية الصحية سيخبرك به؟

الرسائل الاحتيالية المتعلقة بالأعمال التجارية

يستغل المحتالون طبيعة العمل المزدحمة للعديد من الشركات لغشها.

كيفية عمل الرسالة الاحتيالية

تتخذ الرسائل الاحتيالية التي تستهدف الأعمال التجارية جميع الأنواع والأشكال، ومن المرجح أن تضرب في أكثر الأوقات ازدحاماً، مثل نهاية السنة المالية.

الرسائل الاحتيالية بالفواتير الزائفة هي أكثر أنواع الرسائل الاحتيالية شيوعاً والتي يستخدمها المحتالون ضد الشركات. ويقوم المحتالون بإصدار فواتير وهمية بأشياء أو إعلانات أو منتجات أو خدمات غير مرغوب فيها أو غير مُصرح بها. كما إنّ الرسالة **الاحتيالية عبر دليل الأعمال التجارية** هي مثال معروف جيداً، حيث تتلقى فاتورة مقابل إدراج عملك في دليل معروف جيدًا. ويخدعك المحتالون للتسجيل عن طريق إخفاء العرض باعتباره فاتورة مؤجلة أو إدراج مجاني، ولكن تكون هناك اتفاقية اشتراك مخفية مطبوعة بحروف متناهية الصِغر.

الرسالة الاحتيالية المتعلقة باسم نطاق إلكتروني هي حيلة أخرى يستخدمها المحتالون، حيث يتم خداعك عند الاشتراك في تسجيل نطاق إلكتروني غير مرغوب فيه يشبه نطاقك لحدٍ كبير. وقد تتلقى أيضاً إشعاراً بتجديد زائف لاسم نطاقك الفعلي والدفع بدون أن تعرف ذلك.

تنطوي **الرسالة الاحتيالية المتعلقة باللوازم المكتبية** على تلقيك لمنتجات لم تطلبها مع فاتورة مقابل تكلفتها. وغالباً ما يشتمل هذا النوع من الرسائل الاحتيالية على منتجات أو خدمات أنت تطلبها بانتظام مثل القرطاسية ولوازم التنظيف. ويقوم المحتالون عادةً بالاتصال بعملك التجاري مدعين أنه قد تمّ طلب خدمة أو منتج بالفعل.

يقوم المحتال في **الرسالة الاحتيالية المتعلقة بإعادة توجيه الدفع** باستخدام المعلومات التي حصل عليها عن طريق اختراق أنظمة الكمبيوتر الخاصة بك. وبعد ذلك، ينتحل شخصية أحد موردیك المعتادين ويخبرك بأن تفاصيله المصرفية قد تغيَّرت. وقد يخبرك بأنه قام بتغيير البنوك التي يتعامل معها مؤخراً، وقد يستخدم ورقاً مروّساً وعلامات تجارية منسوخة لإقناعك بأنها صحيحة. وسوف يزودك برقم حساب بنكي جديد ويطلب منك إجراء جميع الدفعات المستقبلية وفقاً لذلك. غالباً ما يتم اكتشاف عملية الاحتيال فقط عندما يسأل المورد المعتاد عن سبب عدم الدفع له.

يمكن أن يكون **برنامج الفدية** ضاراً للغاية لأي عمل تجاري. أفضل دفاع هو عمل نسخة احتياطية من بياناتك بانتظام وتخزين النسخ الاحتياطية في ملف خارجي وغير متصل إلكترونياً. اطلع على المزيد من التفاصيل في صفحة 17.

حماية نفسك

- لا توافق على العروض أو الصفقات على الفور - اطلب دائماً تقديم عرض مكتوب واطلب مشورة من جهة مستقلة إذا كانت الصفقة تنطوي على أموال أو وقت أو التزام طويل الأجل.
- لا تقدم أبداً التفاصيل المصرفية والمالية والمحاسبية الخاصة بعملك التجاري إلى شخص يتصل بك بشكل غير متوقع ولا تعرفه وتثق فيه.
- يمكن أن تقطع إجراءات الإدارة الفعالة شوطاً كبيراً في الوقاية من الرسائل الاحتيالية – احرص على وضع اجراءات واضحة للتحقق من الحسابات والفواتير ودفعها، وانظر بعناية شديدة في طلبات تغيير التفاصيل المصرفية.
- قم بتدريب موظفيك على التعرُّف على الرسائل الاحتيالية.
- قم بعمل نسخ احتياطية لبيانات عملك في ملف خارجي وغير متصل إلكترونياً.
- احذر من رسائل البريد الإلكتروني التي تطلب تغييرات على تفاصيل الدفع. تحقق دائماً من التغييرات في تفاصيل الدفع مباشرةً مع الشركة أو الفرد الذي تتعامل معه.

كيفية عمل الرسائل الاحتيالية – شرح آلية الرسالة الاحتيالية

تتبع معظم الرسائل الاحتيالية نفس النمط، وبمجرد فهم ذلك يصبح من السهل اكتشاف حيل المحتال أسهل.

إذا أمعنت النظر في جميع أنواع الرسائل الاحتيالية المختلفة الموضحة في هذا الكتيِّب، فسرعان ما تلاحظ أن معظم الرسائل الاحتيالية تمرُّ بثلاث مراحل: (1) المُفاتحة؛ (2) التواصل؛ و (3) الدفع.

سيساعدك فهم الأجزاء الأساسية للرسالة الاحتيالية على تفادي الانتشار الحالي للرسائل الاحتيالية وحماية نفسك من أية رسائل احتيالية جديدة قد تظهر في المستقبل.

1. المُفاتحة: طريقة الطرح

عندما يُفاتحك المحتالون في الموضوع، فسوف يأتونك دائماً بقصة مصمّمة لتجعلك تصدق كذبة. وسوف يتظاهر المحتال بصفة لا يمتلكها، مثلاً موظف حكومي أو خبير استثماري أو موظف يانصيب أو حتى معجب رومانسي.

لطرح هذه الأكاذيب عيك، سيستخدم المحتالون مجموعة من أساليب التواصل.

إلكترونياً

يتَسَنَّ المحتالون في بيئة مجهولة عبر الإنترنت.

البريد الإلكتروني هو وسيلة مفضلة للطرح، حيث يوفر وسيلة رخيصة وبسيطة للتواصل على نطاق واسع. وتعدُّ رسائل البريد الإلكتروني الاحتيالية التي "تتصيَّد" معلوماتك الشخصية هي أكثر أنواع رسائل البريد الإلكتروني الاحتيالية شيوعاً.

تسمح **منصات الشبكات الاجتماعية ومواقع المواعدة والمنتديات الإلكترونية** للمحتالين "بمصادقتك" والدخول في حياتك الشخصية للوصول إلى بياناتك الشخصية، والتي يمكن استخدامها بعد ذلك ضدك أو مع عائلتك وأصدقائك.

يستخدم المحتالون **مواقع التسوق الإلكتروني والإعلانات المبوبة ومواقع المزادات الإلكترونية** لاستهداف المشترين والبائعين، وغالباً ما يتم الاتصال الأول من خلال مواقع معروفة وموثوق بها أو عبر مواقع إلكترونية وهمية تبدو كأنها حقيقية. ابحث عن خيارات الدفع الآمنة واحذر من طرق الدفع غير المعتادة مثل الحوالة البرقية أو Bitcoins أو البطاقات النقدية مسبقة التغذية. عادةً ما توفر البطاقات الائتمانية بعض الحماية.

عبر الهاتف

يقوم المحتالون بالاتصال هاتفياً ويرسلون رسائلاً هاتفية أيضاً.

يتم إجراء **المكالمات الهاتفية** بواسطة المحتالين إلى المنازل والشركات في مجموعة واسعة من عمليات الاحتيال، بدءاً من تهديد الرسائل الاحتيالية الضريبية إلى عروض الجوائز أو "المساعدة" في مشكلات فيروسات الكمبيوتر. إن توفر مكالمات هاتفية رخيصة عبر بروتوكول التواصل الصوتي عبر الإنترنت (VOIP) يعني أن مراكز الاتصال يمكن أن تعمل من خارج الدولة بأرقام هواتف تبدو كأنها أرقام محلية. ويمكن بسهولة إخفاء هوية المتصل عبر الهاتف وهي واحدة من العديد من الخِدع التي يستخدمها المحتالون لجعلك تصدق أنهم شخص آخر.

يستخدم المحتالون **الرسائل الهاتفية القصيرة (SMS)** لإرسال مجموعة كاملة من الرسائل الاحتيالية بما في ذلك الرسائل المتعلقة بالمسابقات أو الجوائز. وإذا استجبت، فقد يتم محاسبتك بأسعار عالية أو تجد نفسك مشتركاً في خدمة اشتراك. ولكي تكون أكثر أماناً، لا ترد أو تنقر على الروابط في الرسائل النصية إلّا إذا كنت تعرف من أرسلها. ويمكن أن تحتوي هذه الرسائل أيضاً على مرفقات أو روابط لبرامج ضارة تحت ستار صور أو أغاني أو ألعاب أو تطبيقات.

عند بابك

احترس - سيأتي بعض المحتالون إلى باب منزلك مباشرة لمحاولة خداعك.

في **عمليات الاحتيال من الباب إلى الباب،** عادةً يقوم المحتال بالترويج لسلع أو خدمات لا يتم تسليمها أو أنها رديئة للغاية. وقد تحصل حتى على فاتورة عن عمل لم ترغب فيه أو لم توافق عليه. ويتم تنفيذ عمليات الاحتيال من الباب إلى الباب الشائعة من قبل باعة مراوغين يتنقلون من مكان إلى آخر ويقومون بإصلاحات منزلية رديئة أو يأخذون أموالك ويهربون.

يمكن للشركات المقننة أن تبيع من الباب إلى الباب ولكن يجب عليها تحديد هوية موظف البيع والشركة بوضوح واتباع قواعد أخرى. لديك حقوق محددة عندما يتعلق الأمر بممارسات البيع من الباب إلى الباب بما في ذلك فرصة تغيير رأيك - اعرف المزيد عبر www.accc.gov.au/doortodoor.

يمكن أن ينتحل المحتالون شخصيات موظفي **أعمال خيرية مزيفين** لجمع التبرعات. وسوف يستفيدون من أحداث حدثت مؤخراً مثل الفيضانات وحرائق الغابات. قبل التبرع اطلب رؤية الهوية ودفتر الاستلام الرسمي.

لا يزال يتم استخدام **البريد غير المرغوب فيه** لإرسال **رسائل يانصيب ورهان احتيالية وفرص استثمارية والرسائل الاحتيالية النيجيرية ورسائل الميراث المزيفة.** المطبوعة اللامعة ليست ضماناً لمشروعية العرض.

بغض النظر عن طريقة الطرح التي يستخدمونها، تكون قصتهم دائماً هي الطعم وإذا حاولت أخذ قضمة، فسيحاول المحتال نقلك إلى المرحلة التالية.

2. التواصل والاستمالة

إذا منحتهم فرصة للتحدث إليك، فسوف يبدأون في استخدام خِدعاً من صندوق رسائلهم الاحتيالية لإقناعك بدفع أموالك.

يمكن أن تتضمن أدوات المحتال ما يلي:

- يقوم المحتالون بتدوير قصص مدروسة ومقنعة للحصول على ما يريدون.
- يستخدمون **بياناتك الشخصية** لجعلك تعتقد أنك تعاملت معهم في السابق وجعل الرسالة الاحتيال تبدو مشروعة.
- قد **يتواصل معك** المحتال **بشكل منتظم** لبناء الثقة وإقناعك بأنه صديقك أو شريكك أو راغب في بناء علاقة رومانسية معك.
- **يلعبون بمشاعرك** باستخدام الإثارة بالفوز، ووعد بالحب الأبدي، والتعاطف معك في حادث مؤسف، والشعور بالذنب لعدم المساعدة أو القلق والخوف من الاعتقال أو الغرامة.
- يحب المحتالون بثّ **الشعور بالعجلة** حتى لا يكون لديك وقت للتفكير في الأشياء والتفاعل بالعواطف بدلاً من المنطق.
- على نحوٍ مماثل، يستخدم المحتالون **تكتيكات بيع عالية الضغط** ويقولون إن العرض محدود أو الأسعار ستزيد أو أحوال السوق سوف تتغيَّر وسوف تضيع الفرصة.
- يمكن أن تحتوي الرسالة الاحتيالية على جميع السمات المميزة للعمل الحقيقي باستخدام **مطبوعات لامعة** تحتوي على مصطلحات فنية ذات صلة بالمجال المدعومة بواجهات مكاتب ومراكز اتصال ومواقع إلكترونية مهنية.
- مع إمكانية الوصول إلى الإنترنت والبرامج الذكية، من السهل على المحتالين إنشاء **مستندات** مزيفة **وذات مظهر رسمي**. المستند الذي يبدو أنه حصل على موافقة الحكومة أو يحتوي على صياغة غنية بالمصطلحات القانونية يمكن أن يضفي على الرسالة الاحتيالية طابعاً سلطوياً.

أدوات المحتال مصمّمة لإضعاف دفاعاتك والوثوق في القصة والتصرف بسرعة أو بدون عقلانية والمضي قدماً إلى المرحلة النهائية - إرسال الأموال.

3. إرسال المال

أحياناً، تكون طريقة الدفع التي يطلبها المحتال هي أكبر دليل على أن الرسالة احتيالية.

يمكن أن يأتي طلب المال في غضون دقائق من الرسالة الاحتيالية أو بعد أشهر من الاستمالة المتأنية. المحتالون لديهم تفضيلاتهم بشأن كيفية إرسال أموالك.

من المعروف أن المحتالين يقومون بتوجيه الضحايا إلى أقرب موقع **لتحويل الأموال** (مكتب البريد أو خدمة التحويل البرقي أو حتى البنك) لإرسال الأموال. ومن المعروف أنهم يبقون على الهاتف، ويقدمون إرشادات محددة وقد يرسلون حتى سيارة أجرة للمساعدة في ذلك. ويقبل المحتالون الأموال بأي وسيلة، وقد يشمل ذلك **التحويلات البنكية المباشرة أو بطاقات الخصم مسبقة التغذية أو بطاقات الهدايا أو بطاقات Google Play أو Steam أو iTunes** أو العملة الافتراضية مثل **Bitcoin**. أي طلب للدفع بطريقة غير معتادة هو مؤشر على أنه جزء من عملية احتيال.

عادةً ما توفر البطاقات الائتمانية شيئاً من الحماية، ويجب عليك أيضاً البحث عن خيارات الدفع الآمنة التي يظهر فيها "https" في عنوان الموقع الإلكتروني ويحتوي الموقع على رمز قفل مغلق.

لا ترسل مبلغاً مالياً إلى شخص قابلته فقط عبر الإنترنت أو عبر الهاتف - خاصةً إذا كان خارج الدولة.

انتبه إلى أن المحتالين يمكنهم أيضاً المطالبة بالدفع عن طريق سلع ثمينة وهدايا باهظة الثمن مثل المجوهرات أو الإلكترونيات. إن دفع الأموال للمحتالين ليس هو الشيء الوحيد الذي يجب أن تقلق بشأنه - إذا ساعدت في تحويل الأموال لشخص غريب فقد تتورط عن غير قصد في أنشطة **غسيل أموال مخالفة للقانون.**

قواعد ذهبية لحماية نفسك

انتبه لحقيقة وجود الرسائل الاحتيالية. عند التعامل مع متصلين لم تطلبهم من الأفراد أو الشركات، سواء أكان ذلك عبر الهاتف أو بالبريد العادي أو البريد الإلكتروني أو شخصياً أو عبر أحد مواقع التواصل الاجتماعي، فكر دائماً في احتمال أن يكون التواصل عبارة عن رسالة/عملية احتيالية. وتذكر، إذا كان العرض يبدو جيداً بدرجة لا يمكن تصديقها، فمن المحتمل أن يكون احتيالياً.

اعرف مع من تتعامل. إذا قابلت شخصاً عبر الإنترنت فقط أو كنت غير متأكد من شرعية شركة ما، خذ بعض الوقت لإجراء المزيد من البحث، وابحث بالصورة في Google أو ابحث في الإنترنت عن آخرين قد يكون لديهم تعاملات معه.

لا تفتح النصوص المشبوهة أو النوافذ المنبثقة أو رسائل البريد الإلكتروني - امسحها. وإذا لم تكن متأكداً، تحقق من هوية المتصل من خلال مصدر مستقل مثل دفتر الهاتف أو البحث عبر الإنترنت. ولا تستخدم تفاصيل الاتصال الواردة في الرسالة المرسلة إليك.

حافظ على أمان بياناتك الشخصية. ضع قفلاً على صندوق البريد الخاص بك وقم بتمزيق الفواتير والمستندات المهمة الأخرى قبل التخلص منها. احتفظ بكلمات المرور وأرقام التعريف الشخصي في مكان آمن. كن حذرًا بشأن مقدار المعلومات الشخصية التي تشاركها على مواقع التواصل الاجتماعي. يمكن للمحتالين استخدام المعلومات والصور الخاصة بك لإنشاء هوية مزيفة أو لاستهدافك بعملية احتيال.

احذر من طرق الدفع غير المعتادة. غالباً ما يطلب المحتالون الدفع عن طريق التحويلات البنكية والبطاقات مسبقة التغذية وحتى بطاقات Google Play أو Steam أو iTunes و Bitcoin. هذه دائماً مؤشر على أنه جزء من عملية احتيالية.

حافظ على أمان الأجهزة المحمولة وأجهزة الكمبيوتر الخاصة بك. استخدم دائماً حماية لكلمة المرور، ولا تشارك بيانات الدخول مع الآخرين (بما في ذلك الدخول عن بُعد)، وقم بتحديث برامج الأمان والنسخ الاحتياطية للمحتوى. قم بحماية شبكة WiFi باستخدام كلمة مرور وتجنب استخدام أجهزة الكمبيوتر العامة أو نقاط اتصال WiFi للوصول إلى الخدمات المصرفية عبر الإنترنت أو تقديم معلومات شخصية.

اختر كلمات المرور الخاصة بك بعناية. اختر كلمات مرور يصعب على الآخرين تخمينها وقم بتحديثها بانتظام. ويجب أن تتضمن كلمة المرور القوية مزيجاً من الأحرف الكبيرة والصغيرة والأرقام والرموز. لا تستخدم نفس كلمة المرور لكل حساب/ملف شخصي، ولا تشارك كلمات المرور الخاصة بك مع أي شخص.

احذر من أي طلبات للحصول على تفاصيلك أو مالك. لا تقم أبداً بإرسال أموال أو إعطاء أرقام بطاقات الائتمان أو تفاصيل الحساب عبر الإنترنت أو نسخ من المستندات الشخصية لأي شخص لا تعرفه أو تثق فيه. ولا توافق على تحويل أموال أو سلع لشخص آخر: غسيل الأموال يُعدُّ جريمة جنائية.

كن حذراً عند التسوق عبر الإنترنت. احذر من العروض التي تبدو جيدة لدرجة يصعب تصديقها، واستخدم دائماً خدمة التسوق الإلكتروني التي تعرفها وتثق فيها. فكر ملياً قبل استخدام عملات افتراضية (مثل Bitcoin) - فهي لا تتمتع بنفس الحماية التي تتمتع بها طرق المعاملات الأخرى، ما يعني أنه لا يمكنك استرداد أموالك بمجرد إرسالها.

أين تحصل على المساعدة أو الدعم

إذا فقدت أموالك بسبب عملية احتيالية أو قدمت بياناتك الشخصية إلى أحد المحتالين، فمن غير المحتمل أن تسترد أموالك. ومع ذلك، هناك خطوات يمكنك اتخاذها على الفور للحد من الضرر وحماية نفسك من المزيد من الخسائر.

اتصل بالبنك أو الاتحاد الائتماني

إذا قمت بإرسال أموال أو معلومات مصرفية شخصية إلى أحد المحتالين، اتصل بالبنك أو الاتحاد الائتماني الخاص بك على الفور. وقد يستطيعون إيقاف تحويل الأموال أو التحقق منها أو إغلاق حسابك إذا كان لدى المحتال تفاصيل حسابك. وقد تستطيع الجهة التي أصدرت لك البطاقة الائتمانية "ردّ المبلغ" (عكس المعاملة) إذا تمّ خصم مبالغ احتيالية من بطاقتك الائتمانية.

استعادة هويتك المسروقة

إذا كنت تشك في أنك وقعت ضحية لسرقة الهوية، فمن المهم أن تتصرف بسرعة لتقليل خطر الخسارة المالية أو غيرها من الأضرار.

اتصل بـ **IDCARE** - وهي خدمة مجانية تمولها الحكومة وتقدِّم الدعم لضحايا الجرائم المتعلقة بالهوية. ويمكن أن تساعدك IDCARE على وضع خطة استجابة لاتخاذ الخطوات المناسبة لإصلاح الضرر الذي لحق بسمعتك وتاريخك الائتماني وهويتك. قم بزيارة موقع IDCARE الإلكتروني www.idcare.org أو اتصل على الرقم 1300 432 273.

تقدم بطلب للحصول على **شهادة الكومنولث للضحايا** – تساعد هذه الشهادة في دعم مطالبتك بأنك وقعت ضحية لجريمة تتعلق بالهوية ويمكن استخدامها للمساعدة في إعادة إنشاء بيانات اعتمادك لدى الحكومة أو مؤسسات مالية. قم بزيارة موقع دائرة النائب العام (Attorney-General) الإلكتروني www.ag.gov.au (أو اتصل على الرقم 02 6141 6666) لمعرفة المزيد حول حماية هويتك واستعادتها.

اتصل بخدمة مشورة أو دعم

إذا تعرّضت أنت أو أي شخص تعرفه للاحتيال وربما كنت تعاني من التوتر العاطفي أو الاكتئاب، تحدّث إلى الطبيب العمومي أو الأخصائي الصحي بمنطقتك أو أي شخص تثق فيه. ويمكنك أيضاً الاتصال بخدمات مشورة أو دعم، مثل:

Lifeline - عندما تحتاج إلى دعم في أزمة، اتصل بـ Lifeline على الرقم 1114 13 (24 ساعة في اليوم/7 أيام في الأسبوع) أو قم بزيارة www.lifeline.org.au

Beyondblue - للحصول على معلومات حول الاكتئاب أو القلق، اتصل بـ Beyondblue على الرقم 636 224 1300 أو قم بزيارة www.beyondblue.org.au

خط مساعدة الأطفال (Kids helpline) - خدمة مشورة ودعم عبر الهاتف والإنترنت للشباب الذين تتراوح أعمارهم بين 5 و 25 سنة. اتصل بخط مساعدة الأطفال على الرقم 800 551 1800 أو قم بزيارة www.kidshelpline.com.au

الهيئة الأسترالية للمشورة المالية (Financial Counselling Australia) إذا كنت تعاني من ضائقة مالية، اتصل بالرقم 007 007 1800 للتحدث إلى مستشار مالي مجاني أو قم بزيارة www.financialcounsellingaustralia.org.au.

أين تبلغ عن الرسالة الاحتيالية

يمكنك مساعدة الآخرين من خلال إبلاغ الجهات المختصة بالرسالة الاحتيالية. وستساعد معلوماتك هذه المنظمات في تكوين صورة أفضل عن أحدث أنواع الرسائل الاحتيالية وتحذير الآخرين بشأن ما يجب الإنتباه له.

تتلقى المنظمات التالية بلاغات حول أنواع معينة من الرسائل الاحتيالية.

Scamwatch

قم بإبلاغ ACCC عن الرسائل الاحتيالية عبر Scamwatch – قم بزيارة www.scamwatch.gov.au

التفوُّق على المحتالين

تفوَّق على المحتالين - قم بزيارة موقع Scamwatch الإلكتروني للحصول على معلومات حول الرسائل الاحتيالية التي تستهدف المستهلكين الأستراليين والأعمال التجارية الصغيرة. اعرف على المزيد حول كيفية عمل الرسائل الاحتيالية، وكيفية حماية نفسك وما يجب أن تفعله إذا تعرّضت للاحتيال.

اشترك في Scamwatch لتلقي تنبيهات مجانية بالبريد الإلكتروني حول أنواع الرسائل الاحتيالية الجديدة.

www.scamwatch.gov.au

تابع Scamwatch عبر تويتر على scamwatch_gov@ أو http://twitter.com/Scamwatch_gov

إذا تلقيت رسالة احتيالية عبر موقع إلكتروني أو منصة وسائل تواصل اجتماعي، ابلغ عنها إلى الموقع حتى يمكن التحقيق فيها وإزالتها. وإذا قام المحتالون بانتحال شخصية منظمة مقننة مثل دائرة حكومية أو بنك، اخبرهم لكي يتمكنوا من تحذير الآخرين.

وكالات أخرى

يجب عليك أيضاً التفكير في الإبلاغ عن الرسالة الاحتيالية التي تلقيتها إلى وكالات أخرى تتعامل مع أنواع معينة من رسائل احتيالية محدّدة.

نوع الرسالة الاحتيالية	وكالة
جريمة إلكترونية	الشبكة الأسترالية للإبلاغ عن الجرائم الإلكترونية (Australian Cybercrime Online Reporting Network (ACORN)) – قم بزيارة www.acorn.gov.au
الرسائل الاحتيالية المالية والاستثمارية	المفوضية الأسترالية للأوراق المالية والاستثمارات (Australian Securities and Investments Commission (ASIC)) – قم بزيارة www.moneysmart.gov.au أو اتصل بخط معلومات ASIC على الرقم 1300 300 630
الاحتيال والسرقة	الشرطة المحلية - اتصل على 1444 13
البريد الإلكتروني العشوائي والرسائل الهاتفية (SMS)	الهيئة الأسترالية للاتصالات والإعلام (Australian Communications and Media Authority (ACMA)) – قم بزيارة www.acma.gov.au أو اتصل بمركز خدمة عملاء ACMA على الرقم 1300 850 115
الرسائل الاحتيالية المتعلقة بالضرائب	مكتب الضرائب الأسترالي (ATO) - للإبلاغ عن الرسائل الاحتيالية المتعلقة بالضرائب أو التحقق مما إذا كان الشخص الذي يتصل بك موظفاً بالفعل لدى ATO: • اتصل بالرقم 1800 008 540 أو اعد توجيه الرسالة الاحتيالية المتعلقة بالضرائب إلى البريد الإلكتروني ReportEmailFraud@ato.gov.au
الخدمات المصرفية	البنك الذي تتعامل معه أو مؤسسة مالية

اتصل بوكيل حماية المستهلك المحلي

في حين أن ACCC هي الوكالة الوطنية التي تتعامل مع مسائل حماية المستهلك العامة، ثمة وكالات في الولايات والمقاطعتين قد تستطيع أيضاً مساعدتك.

مكتب مقاطعة العاصمة الأسترالية للخدمات التنظيمية (Australian Capital Territory Office of) (Regulatory Services	www.accesscanberra.act.gov.au 13 2281
شؤون المستهلك بفكتوريا (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
نيوساوث ويلز للتجارة العادلة (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
شؤون المستهلكين في المقاطعة الشمالية (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
مكتب كوينزلاند للتجارة العادلة (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
خدمات المستهلك والأعمال التجارية بولاية جنوب أستراليا (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
خدمات المستهلك والبناء والخدمات المهنية في تازمانيا (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
دائرة المناجم وتنظيم الصناعة والسلامة في ولاية غرب أستراليا (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

المزيد من المعلومات

لدى الحكومة الأسترالية بعض الموارد الرائعة حول كيفية الحفاظ على أمانك عبر الإنترنت.

- خدمة الأمان الذكية عبر الإنترنت (Stay Smart Online Service) - www.staysmartonline.gov.au
- موقع CyberSmart - www.cybersmart.gov.au
- أدلة الأمان الذكية عبر الإنترنت (Stay Smart Online guides) - متاحة على www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au