Competition Bureau Canada

Bureau de la concurrence Canada

الكتاب الصغير الأسود عن حالات الاحتيال

Canada

الكتاب الصغير الأسود عن حالات الاحتيال

نشره لأول مرة مكتب المنافسة الكندي عام 2012

هذا المنشور ليس وثيقة قانونية. يتمثل الغرض منه في توفير معلومات عامة للتسهيل عليك.

للحصول على معلومات حول أنشطة مكتب المنافسة، يرجى الاتصال بـ:

Information Centre
Competition Bureau
50 Victoria Street
Gatineau QC K1A 0C9

هاتف: 819-997-4282
الرقم المجاني: 1-800-348-5358
الهاتف النصي (لضعاف السمع): 1-866-694-8389
فاكس: 819-997-0324

موقع الويب: www.competitionbureau.gc.ca

للحصول على نسخة من هذا المنشور، أو استلامه بتنسيق بديل (بطريقة برايل، الطباعة بحروف كبيرة، إلخ.) يرجى الاتصال بمركز معلومات مكتب المنافسة على الأرقام المذكورة أعلاه.

يتوفر هذا المنشور أيضاً عبر الإنترنت بصيغة HTML على الرابط:

http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

الإذن بالنسخ

Cat. No. Iu54-42/2018Ar-PDF
ISBN: 978-0-660-29919-8

مقدمة

المحتالون متسترون وخبثاء يمكنهم استهداف أي شخص، من الصغار إلى المتقاعدين. يمكنهم أيضاً استهداف الشركات التجارية. لا أحد محصن ضد الاحتيال.

وجدت مجموعتنا من الأبطال الخارقين طريقة لاكتشاف عمليات الاحتيال. وسرهم بسيط: المعرفة قوة!

تابع القراءة لمعرفة كيف يمكنك أن تصبح أنت أيضاً بطلاً خارقاً في مكافحة الاحتيال. شارك هذا الكتيب مع أسرتك وأصدقاءك وابدأ بتسليح نفسك بالمعلومات!

فهرس المحتويات

مبادئ مكافحة الاحتيال

كن بطلاً خارقاً حقيقياً عن طريق تسليح نفسك بالمعلومات التي تحتاجها لمكافحة الاحتيال والحفاظ على سلامة نفسك وعائلتك وأموالك.

أنت تعمل بكل جد لكسب أموالك. تود إنفاقها على الأشياء التي تهمك- سواء على تعليم أطفالك أو الذهاب في رحلة مثيرة أو شراء هاتف ذكي جديد.

المحتالون أشخاص حقيقيون. وهم يبحثون في كل يوم عن ضحايا. سيستهدفونك عبر الإنترنت أو عبر الهاتف أو البريد أو شخصياً.

أنت مستهدف. يفقد آلاف الكنديين ملايين الدولارات بسبب المحتالين في كل عام. قد يكون تأثير الاحتيال على العائلات والشركات مدمراً.

تعلم مكافحة الاحتيال. يتضمن هذا الكتيب 12 من أكثر عمليات الاحتيال شيوعا، والتي تستهدف الكنديين حالياً. وهو مليء بالنصائح والحيل حول كيفية حماية نفسك وما عليك فعله إذا تعرضت للاحتيال.

أبلغ عن الأمر! يمكن استهداف أي شخص، من المراهقين، إلى الأجداد، إلى كبار مسؤولي الشركات. أفضل ما يمكنك القيام به هو الإبلاغ عن الاحتيال، مهما كان المبلغ، إلى السلطات المختصة. لا تشعر بالحرج لأن ذلك سيساعد الآخرين على تجنب الوقوع في الفخ نفسه.

المعرفة هي قوتك. احم نفسك بالحصول على مزيد من المعلومات. بالإضافة إلى هذا الكتيب، يمكنك أيضاً استشارة العديد من المواقع الإلكترونية الموثوقة للحصول على مزيد من المعلومات.

لدى المركز الكندي لمكافحة الاحتيال، الذي تديره شرطة الخيالة الكندية الملكية، ومكتب المنافسة، وشرطة مقاطعة أونتاريو، كثير من المعلومات حول الاحتيال. تسلّح بالمعلومات اليوم بزيارة الموقع www.antifraudcentre.ca!

فخاخ الاشتراك

يمكن أن تغريك الصفقات الجيدة للوقوع في فخاخ مكلفة!

يمكن لفخ الاشتراك خداعك عن طريق تقديم تجارب "مجانية" أو "منخفضة التكلفة" للمنتجات والخدمات. عادة ما تكون المنتجات المقدمة حبوب إنقاص الوزن، وأغذية صحية ومستحضرات صيدلانية ومنتجات مكافحة الشيخوخة.

بمجرد تزويدهم ببيانات بطاقة الائتمان الخاصة بك لتغطية تكاليف الشحن، يتم توريطك دون علمك في اشتراك شهري. قد يكون من الصعب، إن لم يكن مستحيلاً تقريباً، إيقاف التسليم ودفع الفواتير.

يستخدم المحتالون مواقع الويب، ورسائل البريد الإلكتروني، ومنصات وسائط التواصل الاجتماعي، والهواتف من أجل الإيقاع بالناس.

تذكر، تستخدم غالباً تكتيكات المبيعات تحت الضغط الشديد مثل "عرض محدود المدة" لدفعك للتسرع في اتخاذ قرار.

نصائح لحماية نفسك:

- **ثق بغرائزك. إذا كان الأمر أروع من أن يصدّق، فلا تقم بالاشتراك.**
- **قبل الاشتراك للحصول على نسخة تجريبية مجانية، اجر بحثاً عن الشركة واقرأ التقييمات النقدية، خصوصاً السلبية منها. يعتبر مكتب تحسين الأعمال مصدراً رائعاً للمعلومات.**
- **لا تشترك إذا لم تتمكن من العثور على الأحكام والشروط أو فهمها. انتبه بشكل خاص إلى المربعات التي تم اختيارها مسبقاً وشروط الإلغاء وسياسات الإرجاع وأي رسوم مبهمة.**
- **إذا اشتركت في تجربة مجانية، احتفظ بجميع المستندات والإيصالات ورسائل البريد الإلكتروني والرسائل النصية.**
- **افحص بانتظام بيانات بطاقة الائتمان الخاصة بك بحثا عن رسوم متكررة أو غير معروفة.**
- **إذا واجهتك مشكلة في إلغاء اشتراكك، اتصل بمزود بطاقة الائتمان، أو منظمة حماية المستهلك المحلية، أو وكالات إنفاذ القانون.**

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

سرقة الهوية

ساعد على ضمان بقاء هويتك خاصة بك وحدك!

يبحث المحتالون دائماً عن كيفية جمع أو نسخ بياناتك الشخصية لارتكاب عمليات الاحتيال. يمكن للصوص إجراء عمليات شراء باستخدام حساباتك، والحصول على جوازات سفر، والحصول على منافع حكومية، والتقدم بطلب للحصول على القروض، وأكثر من ذلك. يمكن لهذا أن يقلب حياتك رأسا على عقب.

يستخدم المحتالون أساليب تتراوح بين طرق غير معقدة إلى تلك البالغة التعقيد. بعيدا عن الإنترنت، يمكنهم البحث في صناديق القمامة أو سرقة البريد. على الإنترنت، يمكنهم استخدام برامج التجسس والفيروسات، بالإضافة إلى القرصنة والتصيد الاحتيالي (انظر صفحة 13).

إنهم يبحثون عن بيانات بطاقات الائتمان، وتفاصيل الحسابات المصرفية، والاسم الكامل والتوقيع، وتاريخ الميلاد، ورقم الضمان الاجتماعي، والعنوان الكامل، واسم الأم قبل الزواج، وأسماء المستخدم وكلمات المرور عبر الإنترنت، ورقم رخصة القيادة ورقم جواز السفر.

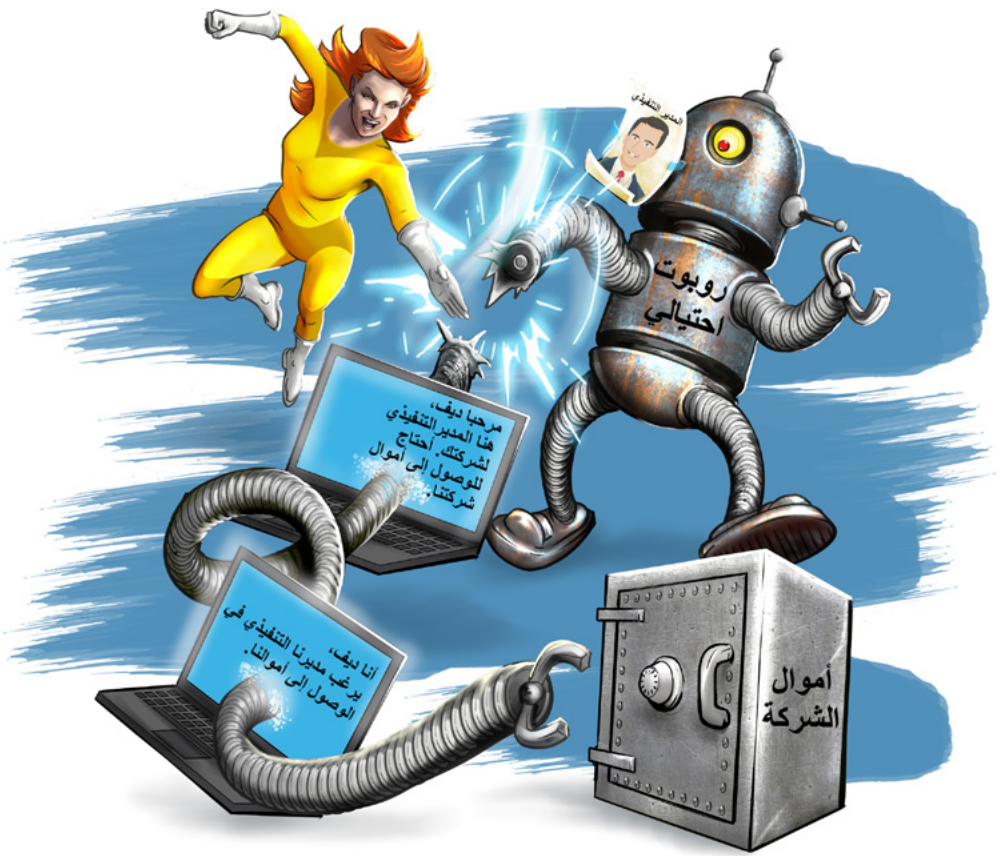
سرقة الهوية هي جريمة خطيرة!

نصائح لحماية نفسك:

- لا تقدم مطلقاً بياناتك الشخصية عبر الهاتف أو عبر الرسائل النصية أو البريد الإلكتروني أو الإنترنت.
- تجنب الحواسيب أو نقاط الاتصال العامة عبر الواي فاي، كما هو الحال في المقاهي، للوصول إلى البيانات الشخصية أو تقديمها؛ فذلك يعرضك للخطر.
- قم بإنشاء كلمات مرور قوية وفريدة لكل من حساباتك على الإنترنت. احم أجهزتك وشبكة الواي فاي المنزلية بكلمة مرور.
- استخدم خدمة دفع آمنة وذات سمعة جيدة عند الشراء عبر الإنترنت، ابحث عن محدد موقع الموارد الموحد URL الذي يبدأ بـ "https" ورمز القفل المغلق.
- تجنب إعطاء بيانات شخصية عبر وسائط التواصل الاجتماعي. فمن الممكن استخدامها مع صورك لارتكاب الاحتيال.
- غطي دائماً رقم تعريفك الشخصي PIN عند استخدام بطاقتك. إذا قمت بتسليمها إلى أمين الصندوق، لا تدعها تغيب عن نظرك.
- مزّق ودمر الوثائق المحتوية على بياناتك الشخصية.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.



عمليات الاحتيال باسم الرئيس التنفيذي

إذا طلب منك الرئيس التنفيذي لشركتك إرسال أموال على وجه السرعة؛ تأكد من أن البريد الإلكتروني حقيقي!

هل تعمل في مجال المحاسبة أو المالية؟ هل لديك السلطة لتحويل الأموال في العمل؟ هل تعمل تحت رئاسة الرئيس التنفيذي (CEO)؟ إذا كانت الإجابة بنعم، كن على حذر؛ فعملية الاحتيال هذه تستهدفك على وجه التحديد!

في حالة نموذجية "للاحتيال باسم الرئيس التنفيذي" ، سينتحل المحتالون شخصية أحد كبار المسؤولين التنفيذيين في الشركة، إما عن طريق الوصول إلى عنوان بريده الإلكتروني أو من خلال تقليده. سيبعثون رسائل بريد إلكتروني تبدو واقعية، والتي تحاول خداعك لتحويل الأموال إلى طرف ثالث.

ستجعل رسائل البريد الإلكتروني الطلب يبدو عاجلاً وسرياً. على سبيل المثال، قد يقولون إن المال مطلوب لإبرام عقد مهم، أو إتمام صفقة سرية، أو تحديث بيانات الدفع الخاصة بأحد الموردين.

عادة ما يكون المحتالون استراتيجيين حول توقيت هذه الرسائل الإلكترونية. فهم يرسلونها عندما يكون المدراء التنفيذيون خارجاً أو يصعب الوصول إليهم. هذه عملية احتيال مربحة قد تكلف الشركات عشرات الآلاف إلى ملايين الدولارات.

يمثل الاحتيال باسم الرئيس التنفيذي تهديدا عالميا متزايدا يستهدف الشركات المحلية الصغيرة والشركات الكبيرة على حد سواء.

نصائح لحماية نفسك:

- **حافظ على أمان الأنظمة الحاسوبية لديك عن طريق استخدام برنامج مكافحة فيروسات محدث وحسن السمعة وكلمات مرور قوية.**
- **تحقق من صحة جميع طلبات التحويل إما عبر الهاتف أو شخصياً. لا تستخدم مطلقاً بيانات الاتصال المقدمة في رسائل البريد الإلكتروني.**
- **تحقق من عنوان البريد الإلكتروني للمرسل- غالباً ما ينشئ المحتالون عناوين تشبه إلى حد كبير العناوين الأصلية، مع اختلاف حرف واحد أو حرفين فقط.**
- **شجِّع شركتك على وضع عملية قياسية لتحويل الأموال، والتي تتطلب مستويات متعددة من الموافقات.**
- **قلّل التفاصيل التي تتشاركها علنا. يستخدم المحتالون المعلومات المتاحة على الإنترنت وعلى شبكات التواصل الاجتماعي للعثور على الضحايا المحتملين وتحديد توقيت الاحتيال عليهم.**

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال الصحية والطبية

احترس من العلاجات السحرية التي تقدم حلولا سريعة وسهلة.

هناك محتالون يأملون استغلال معاناة الناس. الأنواع الثلاثة الأكثر شيوعاً من عمليات الاحتيال الصحية هي العلاجات المعجزة، وبرامج إنقاص الوزن، والصيدليات الوهمية على الإنترنت. في جميع الحالات، غالبا ما تظهر على أنها مشاركات دعائية على مواقع التواصل الاجتماعي أو مواقع الويب المنبثقة.

يعرض المحتالون منتجات وخدمات تبدو كأدوية وعلاجات بديلة أصلية، والتي تعالج الحالات الخطيرة بسرعة وسهولة. قد يبدو أن بعضها حاصل على تأييد بعض المشاهير أو يُروّج له بشهادات من أشخاص يزعمون الشفاء من المرض.

تعطي حيل فقدان الوزن وعوداً بنتائج مذهلة بأقل أو دون مجهود. قد يروج المحتالون لاتباع نظام غذائي غير عادي؛ أو ممارسة تمارين ثورية؛ أو أجهزة للتخلص من الدهون أو منتجات خارقة، مثل الحبوب أو الرقع أو الكريمات.

تقدم صيدليات الإنترنت المزيفة الأدوية والعقاقير بأسعار رخيصة جداً أو بدون وصفة طبية من طبيب. وهي تعلن على الإنترنت وتبعث رسائل البريد الإلكتروني غير المرغوبة. إذا استلمت المنتجات الموعودة بالفعل، فلا يوجد ضمان بأنها أصلية أو آمنة للتناول.

نصائح لحماية نفسك:

- **تذكر أنه لا توجد أقراص سحرية أو علاجات معجزة لتحقيق فقدان الوزن السريع أو لعلاج الحالات الطبية.**
- **لا تثق في الادعاءات المتعلقة بالأدوية والمكملات الغذائية. احصل على الحقائق مباشرة من أخصائي الرعاية الصحية المعالج لك.**
- **لا تلتزم أبداً بأي شيء تحت الضغط، خاصة إذا طلب منك دفعة مسبقة كبيرة أو عقد طويل الأجل.**
- **اعلم أنه لو كانت صيدليات الإنترنت مشروعة، فستتطلب وصفات طبية سارية.**
- **كن متشككا من موافقات أو شهادات المشاهير.**

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال الرومانسية

من يوجد حقا وراء لوحة المفاتيح؟

أبق متيقظاً واحذر من المحتالين المحتملين الذين سيحاولون تخفيض دفاعاتك من خلال استغلال جانبك الرومانسي والعاطفي. يمكنهم تصيّدك على مواقع التعارف الرائجة والأصلية وكذلك على تلك المزيفة.

في موقع المواعدة الحقيقي، قد يرسل لك المحتال بضع رسائل وصورة جيدة المظهر لنفسه/ نفسها أو لشخص ما يدّعي أنه هو/ هي. بمجرد أن تغرم به/ بها، سيبدأ/ تبدأ في مطالبتك بإرسال الأموال. قد يدعون أن أحد أفراد أسرتهم مصاب بمرض شديد أو تعرضهم لموقف عسير يحتاجون إليك فيه لمساعدتكم. بمجرد إعطاءهم المال، غالبا ما يختفون.

يستطيع المحتال أيضاً إنشاء موقع تعارف مزيف، وفيه تدفع مقابل كل رسالة ترسلها وتتسلمها. لحثك على الكتابة والدفع، قد يرسل إليك المحتال رسائل مبهمة بالبريد الإلكتروني عن حبه/ها لك ورغبته/ها فيك.

في كثير من الحالات، قد يرتب المحتال حتى للالتقاء بك شخصيا لجعل عملية الاحتيال تبدو أكثر مصداقية.

نصائح لحماية نفسك:

- لا ترسل الأموال أو تعط أي بيانات مالية عبر موقع تعارف.
- ثق في غرائزك واطرح الأسئلة واقرأ الأحكام والشروط بعناية قبل الاشتراك.
- اعرف أي الخدمات مجانية، وأيها تكلف أموالا، وما يلزم لإلغاء حسابك.
- لا تستخدم سوى مواقع التعارف الأصلية وذات السمعة الجيدة. تحقق دائماً من عناوين مواقع الويب بعناية، حيث إن المحتالين يقلدون في كثير من الأحيان عناوين الويب الحقيقية.
- تذكر أنه من غير المحتمل على الإطلاق أن يصرح شخص بحبّه الأبدي لأي شخص بعد تبادل عدد قليل من الرسائل أو رسائل البريد الإلكتروني أو المكالمات الهاتفية أو الصور.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال على الشركات

ابق على اطلاع على المخططات التي تستهدف الشركات!

يمكن حتى خداع المنظمات من أي حجم بطرق الاحتيال الذكية، لذلك تأكد من التعرف عليها.

من النماذج الشهيرة عملية الاحتيال عبر الدليل. يرسل المحتال إلى شركتك مقترحاً للإدراج أو الإعلان في مجلة أو جريدة أو دليل أعمال أو دليل على الإنترنت. سيتصل هاتفيا لتأكيد العنوان وغيره من البيانات، وبعد ذلك سيتسلم قسم المحاسبة الفاتورة ويدفعها، غير مدرك بأنّ شركتك لم تطلب الخدمة أو تأذن بها في الواقع.

هناك احتيال شائع آخر، وهو الاحتيال المتعلق بمنتجات الصحة والسلامة. قد تتلقى مكالمة هاتفية من شخص يدعي أنه من حكومة المقاطعة، ويخبرك بأن حقيبة الإسعافات الأولية الخاصة بشركتك تحتاج إلى استبدال أو أن عليك تحديث تدريب شركتك في مجال الصحة والسلامة. في كلتا الحالتين، قد يُطلب منك التصرف بسرعة.

هناك احتيال آخر محتمل، وهو الاحتيال المتعلق بالتجهيزات المكتبية، والذي ينطوي على تلقي ودفع ثمن سلع لم تطلبها.

في كثير من الحالات، سيطاردك المحتالون لدفع المبلغ الذي يدعون بأنك مدين لهم به. حتى أنهم سيخدعونك لتصدق بأنهم سيبلغون عنك إلى وكالة للتحصيل.

نصائح لحماية نفسك:

- ثقّف نفسك وموظفيك وزملائك في العمل بتوخي الحذر من المكالمات غير المرغوب فيها.
- أنشئ قائمة بالشركات التي تتعامل معها شركتك عادة.
- قلل عدد الموظفين الذين يمكنهم الموافقة على المشتريات ودفع الفواتير.
- حدد بوضوح إجراءات التحقق والدفع وإدارة الحسابات والفواتير.
- اتصل بمسؤول التنظيم في المقاطعة لمعرفة التزاماتك القانونية.
- سيستخدم المحتالون أسماء شركات أو شعارات مشابهة لتلك الخاصة بالشركات المعروفة لجعل فواتيرهم تبدو حقيقية. افحص الفواتير بعناية قبل دفع أي مبالغ.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

التصيد الاحتيالي وعمليات الاحتيال عبر الرسائل النصية

كن على حذر. يمكن تلفيق الرسائل بسهولة!

بالنظر إلى أننا نقضي المزيد من الوقت على الإنترنت، يزداد المحتالون ابتكارا في عمليات الاحتيال عبر الفضاء الرقمي.

يحدث التصيد الاحتيالي عندما تتسلم رسالة غير مرغوب فيها بالبريد الإلكتروني، والتي يدعي مرسلها أنه من منظمة ذات ترخيص، مثل المؤسسات المالية أو الشركات أو الوكالات الحكومية. يطلب منك المحتالون تقديم أو تأكيد، إما عبر البريد الإلكتروني أو بالنقر على رابط للويب، بياناتك الشخصية أو المالية، مثل رقم بطاقة الائتمان الخاصة بك، وكلمات المرور ورقم الضمان الاجتماعي.

الاحتيال عبر الرسائل النصية هو الشيء نفسه، إلا أنه يتم عن طريق الرسائل النصية.

غالباً ما تنسخ هذه الرسائل أسلوب وشعار المؤسسات التي تثق بها، وعادة ما تتضمن دعوة إلى اتخاذ إجراء ما. وهي تتخذ العديد من الأشكال والنماذج، لكنها في النهاية تسعى للحصول على بياناتك الشخصية.

نصائح لحماية نفسك:

- اعلم أن المنظمات ذات السمعة الطيبة لن تطلب أبداً بياناتك الشخصية عن طريق البريد الإلكتروني أو الرسائل النصية.
- تجاهل الرسائل الواردة من جهات اتصال غير معروفة.
- قم بحذف الرسائل المشبوهة لأنها قد تحمل الفيروسات.
- لا ترد على رسائل البريد غير المرغوبة، ولو حتى لإلغاء الاشتراك، ولا تفتح أي مرفقات أو تتبع أي روابط.
- للتحقق من ارتباط تشعبي دون النقر عليه، مرر مؤشر الفأرة فوقه. تحقق بعناية مما إذا كان صحيحا.
- قم بتحديث برنامج مكافحة الفيروسات الخاص بك على جميع الأجهزة.
- لا تستخدم مطلقاً رقم الهاتف أو عنوان البريد الإلكتروني الوارد في الرسالة المريبة- استخدم بيانات الاتصال المدرجة على مواقع الويب التي تم التحقق منها.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال الضريبية

هل تلقيت مكالمة أو بريد إلكتروني من وكالة الإيرادات الكندية (CRA)؟ تأكد من صحتها!

تتلقى رسالة نصية أو رسالة بريد إلكتروني من وكالة الإيرادات الكندية تدعي بأنه يحق لك استرداد مبلغ إضافي وأن كل ما عليك القيام به هو تقديم بياناتك المصرفية. احترس- هذا الوضع الرائع- إذا كان صحيحا- هو بالضبط ما تبدو عليه عملية الاحتيال الضريبي.

هناك صيغة أخرى، وهي الاتصال بك والادعاء بأنك مدين بأموال لوكالة الإيرادات الكندية وأن عليك دفعها على الفور، وإلا فسيبلغون الشرطة.

على أية حال، إذا تلقيت مكالمة أو رسالة أو بريداً إلكترونياً أو رسالة نصية تذكر أنك مدين بمال لوكالة الإيرادات الكندية ، يمكنك التحقق عبر الإنترنت عن طريق خدمة "حسابي" My Account أو الاتصال بالرقم 1-800-959-8281.

نصائح لحماية نفسك:

لن تقوم وكالة الإيرادات الكندية أبداً بما يلي:

- استخدام لغة عدوانية أو تهديدية.
- تهديدك بالاعتقال أو إرسال الشرطة.
- طلب الدفعات عبر بطاقات الائتمان المدفوعة مسبقاً أو بطاقات الهدايا، مثل آي تيونز وهوم ديبو وما إلى ذلك.
- جمع أو توزيع المدفوعات عن طريق التحويل الإلكتروني Interac e-transfer.
- استخدام الرسائل النصية للتواصل تحت أي ظرف من الظروف.

رسائل البريد الإلكتروني الواردة من وكالة الإيرادات الكندية:

- لا تطلب أبدا بيانات مالية.
- لا تقدم أبدا بيانات مالية.

طرق الدفع المقبولة لدى وكالة الإيرادات الكندية هي:

- الخدمات المصرفية عبر الإنترنت.
- بطاقة الخصم.
- الخصم المخوّل مسبقاً.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال من الباب إلى الباب

طق، طق! من هناك؟ محتال!

على الرغم من أننا نعيش في العصر الرقمي، لا تزال هناك بعض عمليات الاحتيال القديمة التي تأتي مباشرة إلى باب منزلك، مما يشكل تهديدا لك وللشركات. في عمليات الاحتيال هذه، يستخدم مندوبو المبيعات بطريقة الباب إلى الباب تكتيكات تحت ضغط شديد لإقناعك بشراء منتج أو الاشتراك للحصول على خدمة لا تريدها أو تحتاج إليها.

غالباً ما تكون هذه الخدع العدوانية للتبرعات الخيرية، أو فرص الاستثمار أو الخدمات المنزلية وصيانة الأجهزة المختلفة، مثل سخانات المياه والأفران ومكيفات الهواء.

في كثير من الحالات، لن تتلقى أبداً المنتج أو الخدمة التي وعدت بها. في أحيان أخرى، تكون المنتجات أو الخدمات ذات نوعية رديئة أو ليست كما عُرض عليك.

نصائح لحماية نفسك:

- لا تشعر بالضغط لاتخاذ قرار سريع- خذ وقتك لإجراء بعض البحث حول البائع والمنتجات أولاً.
- اطلب بطاقة هوية تحمل صورة، واعرف اسم الشخص والشركة أو المؤسسة الخيرية التي يمثلها.
- اطلب تفاصيل عن المؤسسة الخيرية حول كيفية تخصيص الأموال. تأكد من الحصول على هذا كتابياً.
- لا تشارك أي بيانات شخصية أو نسخ من أي فواتير أو كشوفات مالية.
- لا تسمح بالدخول إلى عقارك إلا للأشخاص الذين تثق بهم. قبل أن تستثمر.
- قم بالبحث قبل أن تستثمر. لا توقع على أي شيء واقرأ دائما التفاصيل الدقيقة.
- اعرف حقوقك. اتصل بمكتب شؤون المستهلك المحلي- معظم المقاطعات والأقاليم لديها مبادئ توجيهية بموجب قانون حماية المستهلك.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

عمليات الاحتيال بادعاء حالات الطوارئ

أيها الأجداد المحبون، لا تتصرفوا بسرعة كبيرة!

عادة ما تستهدف عمليات الاحتيال بادعاء حالات الطوارئ الأجداد المحبين، وذلك باستغلال عواطفهم لسرقة أموالهم.

تبدأ عملية الاحتيال النموذجية بتلقي الجد أو الجدة لمكالمة هاتفية من شخص يدعي أنه حفيده/ حفيدها. يتابع "الحفيد" القول بأنه في ورطة- تشمل المحن الشائعة تعرضه لحادث سيارة أو حبسه في السجن أو وجود مشكلات في العودة إلى الوطن من بلد أجنبي- وأنه بحاجة المال على الفور.

سيطرح عليك المتصل أسئلة، مما يجعلك تكشف عن بياناتك الشخصية. سيجعلك أيضاً تقسم على السرية، فيقول إنه يشعر بالحرج ولا يريد أن يكتشف أفراد العائلة الآخرين ما حدث.

ينطوي نوع آخر من هذه الحيلة على وجود شخصين على الهاتف، يتظاهر أحدهما بأنه الحفيد والآخر بأنه ضابط شرطة أو محام.

في حالات أخرى، سيتظاهر المحتال بأنه جار قديم أو صديق للعائلة في ورطة.

نصائح لحماية نفسك:

- خذ وقتك للتحقق من القصة. يعتمد المحتالون على رغبتك في المساعدة السريعة للشخص العزيز عليك الواقع في حالة طارئة.
- اتصل بوالدي الطفل أو أصدقائه لمعرفة مكانه.
- اطرح على المتصل أسئلة لا يمكن سوى للشخص الذي تعرفه الإجابة عليها، وتحقق من هويته قبل اتخاذ خطوات للمساعدة.
- لا ترسل الأموال إلى أي شخص لا تعرفه وتثق به.
- لا تقم أبدا بإعطاء أي بيانات شخصية للمتصل.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

الاحتيال عن طريق شراء البضائع

لا يتمتع جميع البائعين عبر الإنترنت بسمعة طيبة!

يمثل التسوق عبر الإنترنت تسلية مفضلة لكثير من المستهلكين. لكن العديد من الصفقات التي تراها على الإنترنت- من المحافظ الأصلية الرخيصة إلى السلع الإلكترونية المخفضة بشكل كبير- هي أروع من أن تكون حقيقية.

قد ينشئ المحتالون حسابات على مواقع المزادات المعروفة، مثل eBay، أو على سوق عبر الإنترنت، مثل Kijiji أو Craigslist. سيعلنون عن منتجاتهم بأسعار منخفضة للغاية، مما يحفزك على شرائها.

في نهاية المطاف، إذا حصلت على أي شيء، فقد يكون ذا نوعية رديئة أو تقليد سيئ لما توقعته.

في حالات أخرى، سيغريك المحتالون بالنقر على روابط لجهات راعية ستوجهك إلى موقع للويب يبدو حقيقيا. إذا قررت الشراء من هناك، فلن تستفيد من أي حماية أو خدمات تقدمها المواقع المشروعة.

إذا كان الموقع أو العرض متميزاً بشكل كبير عن البقية، فمن المحتمل وجود حيلة ما.

نصائح لحماية نفسك:

- اشتر من الشركات أو الأفراد الذين تعرفهم عن طريق السمعة أو من تجارب سابقة.
- لا تبرم صفقة أبدا خارج موقع المزاد.
- حذار من البائعين البعيدين أو الذين لديهم تقييمات نقدية محدودة أو معدومة.
- استخدم بطاقة ائتمان عند التسوق عبر الإنترنت؛ يقدم العديد منها حماية وقد يرد أموالك.
- كن حذراً من مواقع الويب التي تحتوي على أخطاء إملائية وأخطاء نحوية.
- اقرأ سياسات استرداد الأموال وإرجاع البضائع، بما في ذلك التفاصيل الدقيقة.
- اطرح على الموردين أسئلة وتأكد من الجداول الزمنية لتقديم الخدمات والتكلفة الإجمالية.

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

الاحتيال عن طريق بيع البضائع

يمكن أن يظهر المحتالون كمشترين.

إذا كنت تبيع سلعاً عبر الإنترنت، إما بشكل شخصي أو كجزء من نشاط تجاري، كن على حذر من المشتري، حيث أن هناك خطر التعرض للاستهداف من قِبل المحتالين الذين يرغبون في أخذ سلعك أو نقودك أو كلاهما.

في إحدى الصيغ، سيوافق المحتال على شراء بضاعتك دون رؤيتها. ستحصل على إشعار مالي من PayPal أو بالبريد الإلكتروني يدعي أن الدفعة في انتظار المراجعة.

تكمن الخدعة في أن الإشعار سيقول أنه لن يتم إصدار الدفعة إلا عند تقديم رقم تتبع للبضائع. عند إدخالك لرقم التتبع، ستكون قد شحنت البضائع بالفعل، ووقتها ستعرف أن إشعار الدفع كان مزيفاً.

في حالات أخرى، قد يُدفع لك عن طريق تحويل نقدي مزيف أو شيك احتيالي أو بطاقة ائتمان مسروقة.

في صيغة أخرى، قد يرسل لك المحتال رسالة تفيد بأنه لا يمكن إرسال الدفعة بسبب مشكلة في حسابك على PayPal أو حسابك المصرفي. سيُطلب منك دفع رسوم للحصول على حساب للشركات لإكمال المعاملة. سيعرض المحتال دفع الرسوم إذا قمت بتسديدها له باستخدام خدمة لتحويل الأموال أو إرسال الحوالات. إذا وافقت، فستذهب أموال "الرسوم" إلى الفنان المحتال.

نصائح لحماية نفسك:

- **اجتمع دائماً في مكان محلي وعام ومأمون لإتمام مبادلة.**
- **حذار من رسائل البريد الإلكتروني العامة ذات الأخطاء النحوية.**
- **حذار من المشترين البعيدين الذين يرغبون في شراء منتجات أو أشياء أخرى دون رؤيتها.**
- **تحقق من عنوان البريد الإلكتروني للمرسل- غالباً ما ينشئ المحتالون عناوين تشبه إلى حد كبير العناوين الأصلية، مع اختلاف حرف واحد أو حرفين فقط.**
- **لا ترسل أموالا للحصول على المال.**

إذا شككت في عملية احتيال، أبلغ عنها دائماً.

انتقل إلى الصفحتين 19 و20 لمزيد من المعلومات.

علامات التحذير: أمور يجب الانتباه لها

تعلم التعرف على العلامات التي تدل على وجود خطأ ما.

الحوالات المصرفية. تتضمن العديد من عمليات الاحتيال طلباً لإرسال الأموال إلكترونياً باستخدام خدمة لتحويل الأموال، مثل موني غرام MoneyGram وويسترن يونيون Western Union، أو باستخدام عملة مشفّرة مثل بيتكوين. تذكر أن إرسال حوالة عبر هذه الخدمات يشبه إرسال الأموال نقداً- بمجرد استلام المبلغ، فمن شبه المستحيل استرداد أموالك.

المدفوعات الزائدة. عندما تبيع شيئاً- خصوصاً عبر الإنترنت- كن حذراً من كيفية الدفع لك. قد يرسل لك المحتال شيكا مزيفا من أمين الصندوق، إما شخصي أو تجاري بمبلغ يتجاوز ما يدين لك به. سيُطلب منك إيداع الشيك وتحويل الأموال الزائدة فوراً إليهم. بمجرد أن يدرك البنك أن الشيك مزور، ستكون مسؤولا عن الأموال المسحوبة.

الأخطاء الإملائية. كن متشككا من رسائل البريد الإلكتروني أو الرسائل أو المواقع التي تحتوي على كلمات شائعة بها أخطاء إملائية؛ أو أخطاء نحوية تجعل من الصعب قراءتها أو تعابير مستخدمة بشكل غير صحيح. يجب أيضاً تفحص عناوين البريد الإلكتروني وعناوين الويب بدقة لمعرفة ما إن كانت هناك أخطاء أو اختلافات طفيفة.

طلب البيانات الشخصية. قد يطلب المحتالون من الضحايا المحتملين تقديم بيانات شخصية أو مالية أكثر مما هو مطلوب للمعاملة أو المناقشة. كن متشككاً إذا طلب منك أحدهم نسخاً من جواز سفرك أو رخصة القيادة أو رقم الضمان الاجتماعي أو تاريخ الميلاد، خاصة إذا كنت لا تعرف من يطلبها.

المكالمات غير المرغوب فيها. قد تتلقى مكالمة من شخص يدعي أن لديك فيروس على حاسوبك، أو أنك مدين للضرائب أو أنه وقع نشاط احتيالي في حساباتك المصرفية. اعلم أن المؤسسات المشروعة لن تتصل بك مباشرة. قم بإنهاء المكالمة واتصل بالمؤسسة بنفسك باستخدام الرقم المستقى من مصدر موثوق به، مثل دفتر الهاتف أو موقع الويب الخاص بالمؤسسة أو حتى الفواتير وكشوف الحساب.

طلبات الصداقة غير المرغوب فيها على شبكات التواصل الاجتماعي. لا تقبل طلبات صداقة من أشخاص لا تعرفهم حتى تراجع ملفهم الشخصي أو تسأل أصدقاءك الحقيقيين ما إن كانوا يعرفونهم. هل يبدو ملفهم الشخصي فارغاً إلى حد ما أم أنه يحتوي على مشاركات عامة للغاية؟ هل يبدو أنه يعد بأكثر من الصداقة؟ هذه بعض العلامات التحذيرية التي تشير إلى عملية احتيال. احذف هذا الطلب وقم بحظر الطلبات المستقبلية.

العروض البريدية المذهلة. لقد تلقيت بطاقة لعبة في البريد، والتي تضمن لك الفوز أو أنك فزت بالفعل. قد تتراوح الجوائز من السيارات إلى الرحلات. إذا لم تكن قد شاركت في مسابقة، تخلص من هذه البطاقة، فهي على الأرجح عملية احتيال!

إن ذلك فقط أروع من أن يصدّق. كلنا يحب الحصول على صفقة رائعة. لكن العروض الصادمة، والخصومات المذهلة، والأسعار غير الحقيقية قد تدل على أن العرض ليس كما يبدو تماماً. عادة ما تشتري الأسعار الرخيصة منتجات رخيصة، أو سلع مزيفة. قد تتطلب العروض المجانية منك تقديم بيانات بطاقة الائتمان الخاصة بك من أجل الشحن. يمكن أن تؤدي تكتيكات صغيرة كهذه إلى أرباح كبيرة للمحتالين.

الإبلاغ عن عملية احتيال

يعتمد الشخص الذي يتعين عليك الاتصال به على المكان الذي تعيش فيه ونوع عملية الاحتيال.

سواء تعرضت لعملية احتيال أو تم استهدافك من قبل محتال، يجب عليك دائما الإبلاغ عن ذلك. قد لا تتمكن السلطات الكندية دائماً من اتخاذ إجراء ضد عمليات الاحتيال، لكن هناك طرق يمكنك المساعدة بها. عن طريق الإبلاغ عن عملية الاحتيال، قد تتمكن السلطات من تحذير الأشخاص الآخرين وتنبيه وسائل الإعلام لتقليل فرص انتشار عملية الاحتيال. عليك أيضاً تحذير أصدقائك وأسرتك من أي عمليات احتيال قد تصادفك.

فيما يلي بعض النصائح حول جهة الإبلاغ، بناء على نوع عملية الاحتيال:

المركز الكندي لمكافحة الاحتيال
www.antifraudcentre.ca
1-800-495-8501

مكتب المنافسة
www.competitionbureau.gc.ca
1-800-348-5358

عمليات الاحتيال المحلية

اتصل بمكتب شؤون المستهلك المحلي

يعد مكتب شؤون المستهلك المحلي في منطقتك أفضل مصدر للتحقيق في عمليات الاحتيال التي يبدو أنها تأتي من داخل المقاطعة أو الإقليم الذي تعيش فيه. يمكن العثور على قائمة بمكاتب شؤون المستهلك على مستوى المقاطعات والأقاليم في دليل المستهلك الكندي.

www.consumerhandbook.ca

عمليات الاحتيال المالية والاستثمارية

اتصل بالمسؤولين عن الأوراق المالية الكندية

تتضمن عمليات الاحتيال المالية عروض مبيعات أو عروضا ترويجية حول المنتجات والخدمات المالية، مثل التقاعد، أو الصناديق المدارة، أو الاستشارات المالية، أو التأمين، أو حسابات الائتمان أو الودائع.

تشمل عمليات الاحتيال الاستثمارية شراء الأسهم، وتداول العملات الأجنبية، والاستثمارات الخارجية، ومخططات بونزي، أو خطط الاستثمار في البنوك الرئيسية.

يمكنك الإبلاغ عن عمليات الاحتيال المالية والاستثمارية لمديري الأوراق المالية الكندية أو منظم الأوراق المالية المحلي في منطقتك.

www.securities-administrators.ca

عمليات الاحتيال المصرفية وبطاقات الائتمان

اتصل بالبنك أو المؤسسة المالية التي تتعامل معها

بالإضافة إلى الإبلاغ عن عمليات الاحتيال هذه إلى مركز مكافحة الاحتيال الكندي، يجب عليك تنبيه البنك أو المؤسسة المالية حول أي مراسلات مشبوهة تتلقاها بخصوص حسابك. يمكنهم تقديم النصح بشأن ما يجب فعله بعد ذلك.

عند الاتصال ببنكك أو مؤسستك المالية، تأكد من استخدام رقم الهاتف الموجود في دفتر الهاتف، أو في كشف حسابك أو على ظهر بطاقتك.

رسائل البريد الإلكتروني والرسائل النصية غير المرغوب فيها

اتصل بمركز الإبلاغ عن الرسائل غير المرغوب فيها

يصل العديد من عمليات الاحتيال عبر البريد الإلكتروني والرسائل النصية. قم بزيارة www.fightspam.gc.ca للحصول على معلومات حول التشريع الكندي لمكافحة البريد المزعج وكيفية التبليغ عنه.

يمكن أيضاً إبلاغ البنك أو المؤسسة المالية أو غيرها من المؤسسات المعنية بالرسائل الاحتيالية أوالتصيدية التي تطلب تفاصيل شخصية . مرة أخرى، تأكد من استخدام رقم هاتف أو عنوان بريد إلكتروني مدرج في مصدر رسمي معروف، وليس العنوان الذي يظهر في البريد الإلكتروني.

الاحتيال والسرقة والجرائم الأخرى

اتصل بالشرطة

كثير من عمليات الاحتيال التي قد تنتهك قوانين حماية المستهلك (تلك التي يفرضها مكتب المنافسة وغيره من الأجهزة الحكومية ووكالات إنفاذ القانون) قد تنتهك أيضاً أحكام الاحتيال في القانون الجنائي.

إذا وقعت ضحية لعملية احتيال- بمعنى أنك تكبدت خسارة بسبب عدم أمانة أو خداع شخص ما- فكر في الاتصال بالشرطة المحلية، خاصة إذا كان المبلغ المعني كبيرا. يجب عليك بالتأكيد الاتصال بالشرطة إذا سُرقت ممتلكاتك أو تعرضت للتهديد أو الاعتداء من قبل محتال.

سرقة الهوية

اتصل بالشرطة

تشير سرقة الهوية إلى الحصول على بيانات شخصية لشخص آخر وجمعها لأغراض إجرامية.

إذا شككت أو علمت أنك ضحية لسرقة الهوية أو الاحتيال، أو إذا قمت دون قصد بتقديم بياناتك الشخصية أو المالية، فيجب عليك:

- الاتصال بقوات الشرطة المحلية وتقديم بلاغ.
- اتصل بالبنك أو المؤسسة المالية و الشركة المصدرة لبطاقة الائتمان.
- اتصل بمكتبي الائتمان الوطنيين وسجل إخطار بوقوع الاحتيال على تقارير الائتمان الخاصة بك.
- قم دائما بالإبلاغ عن سرقة الهوية والاحتيال. اتصل بالمركز الكندي لمكافحة الاحتيال.

منظمات إضافية للاتصال بها حسب الحالة:

- مكتب تحسين الأعمال في المقاطعة
- وكالة الإيرادات الكندية- خط الاستعلام عن الجهات الخيرية

www.cra-arc.gc.ca
1-800-267-2384

- مكتب سجلات المقاطعة التي تعيش فيها
- يمكن لمكاتب الائتمان إصدار إخطار بوقوع احتيال على حسابك، مما ينبه المقرضين والدائنين بوقوع احتيال محتمل:

إكويفاكس كندا Equifax Canada
1-800-465-7166

ترانسيونيون كندا TransUnion Canada
1-866-525-0262

يتوفر الكتاب الصغير الأسود عن حالات الاحتيال على الإنترنت على الموقع
www.competitionbureau.gc.ca

المعرفة قوة!