نصائح للاشخاص البالغين بخصوص النصب والاحتيال والامان الالكتروني

مكالمات احتيال هاتفية:

خذ حذرك من المتصلين المدعين بانهم يمثلون شركة معروفة او منظمة مشهورة

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdlnt-clls-en.aspx

ماذا تفعل اذا استلمت هذه النوعية من المكالمات :

اقفل الخط ولا تعطي اي معلومات عن بعد للسماح بالدخول الى معلوماتك الالكترونية لاي متصل غير معلوم. اذا لم تكن متأكدا اتصل بخدمة العملاء للشركة او المنظمة المتصلة , ننصحك بشدة ان تقوم بالابلاغ عن هذه الحوادث للمركز الكندي لمكافحة الاحتيال او الاتصال برقم 1888 495 8501

ولمن يعانون من صعوبات في السمع الاتصال على الرقم 1800 926 9105

النصب والاحتيال الالكتروني:

ليس من السهل التحقق من اذا كان البريد الالكتروني او العرض المقدم حقيقيين او نصب واحتيال الكتروني , قد يكون العرض مغري لدرجة يصعب تصديقه وقد يكون صادق , المفتاح هنا هو ملاحظة علامات التفنن في النصب والاحتيال.

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx

اين استطيع ان اتعلم المزيد ؟

هناك العديد من المصادر الالكترونية الجيدة للمعلومات حول النصب والاحتيال

https://www.canada.ca/en/financial-consumer-agency.html

تعطي معلومات حول حقوقك في التعامل مع البنوك او اي مؤسسات مالية اخرى.

لطلب نسخ اضافية من هذا المنشور او لطلب مساعدة في ايجاد رقم هاتف في مقاطعتك او منطقتك اتصل على الرقم 1800 622 6232

1800 926 9105

Translated by Abeer Hattab

ماذا يجب ان افعل عندما اشك باني تعرضت للنصب والاحتيال ؟

اكثر حالات النصب شيوعا هي الخداع والتلاعب.

اكثر حالات النصب شيوعا في كندا :

عندما يظهر المحتال وكانه صاحب عمل او منظمة حكومية , ومتال على هذه الحالة عندما يتظاهر المتصل بانه يمثل وكالة الدخل القومي الكندي.

احيانا يتم ابلاغ الضحايا بانهم مدينين للوكالة بمبلغ من المال واذا لم يقوموا بالدفع فانه سيتم القبض عليهم من قبل الشرطة.

واحيانا اخرى يخبر الضحايا بانه بامكانهم الضغط على رابط للحصول على مردوداتهم من الحكومة .

واحيانا يتم ابلاغ الضحايا باتباع رابط معين لمراجعة بعض التغييرات او ان يطلب منهم تعبئة نماذج تتضمن معلوماتهم الشخصية.

اذا لم تكن متاكدا من صحة الرسالة لا تقم بالرد عليها افتح على الصفحة الالكترونية للمنظمة او قم بالاتصال بهم هاتفيا للتاكد من صحة ما وصل اليك من رسائل .

الكثير منا استلم اتصالات وايميلات من دائرة الدخل القومي الكندي تامرنا بدفع مبالغ مالية مترتبة علينا للضرائب' الوكالة تقدم النصائح التالية:

وكالة الدخل القومي الوطني لا تطالب بمعلومات شخصية عبر البريد الالكتروني اوالرسائل النصية

الدائرة لا تقبل الدفع بعملة البيتكوين او كروت الهدايا

اذا استلمت رسالة نصية او رسالة الكترونية بانك مدين للحكومة بمبالغ مالية او ان الحكومة مدينة لك بمبالغ مالية او امتيازات ادخل الى حسابك الالكتروني او حساب عملك الالكتروني لتطلع على وضعك الضريبي او اتصل برقم الاستفسارات حول الضرائب الشخصية للافراد 1800 959 8281

اذا تم بالفعل الاحتيال عليك هناك مجموعة من الخطوات يجب اتخاذها:

1 اتصل بالشرطة المحلية التابعة لمنطقتك شرطة بيرنابي للحالات **غير الطارئة (24 ساعة)** على الرقم 604 646 9999 او الصفحة الالكترونية

http://burnaby.rcmp-grc.gc.ca

2 اذا تم سرقة رقمك الوطني يجب ان تتواصل مع خدمات كندا (سيرفس كندا)

على الرقم 1800 206 7218

3 بلغ عن الاحتيال الذي تعرضت له للمركز الكندي لمكافحة الغش , قد يطلب منك ان تدخل الى حسابك الالكتروني عن طريق شريك اخر (كالبنك الذي تتعامل معه) يمكنك الاتصال على المركز على الرقم 1888 495 8501

المحتالين يتبعون نفس الاسلوب عند التظاهر بانهم يمثلون بنك او شركة كروت ائتمانية .

قد يصلك بريد الكتروني من بنك لا تتعامل معه اصلا يخبروك بمراجعة حسابك الشهري , وهنا يكون من السهل اكتشاف الاحتيال لانك لا علاقة لك بهذا البنك . لكن اذا كان عندك شك بان هذه الرسالة قد تكون من بنكك لا تقم بالرد عليها الكترونيا , تواصل مع بنكك مباشرة او ادخل على حسابك الكترونيا من اجهزة موثوق منها للتحقق من وضعك المادي وبكل الاحوال تواصل مع البنك الذي تتعامل معه.

للمزيد من المعلومات عن حوادث الاحتيال وطريقة التبليغ عنها قم بزيارة الموقع الالكتروني

https://www.cyber.gc.ca/en/cyber-incidents

5 طرق لحماية خصوصياتك على الاجهزة الذكية (التلفونات الذكية اجهزة التابلت الساعات الذكية)

هذه النصائح تخص اي جهاز متصل بالانترنت في بيتك , استعمال الاجهزة الذكية ممتع ويسهل الحياة الا انها قد تمنح الفرصة للقراصنة بان يصلوا الى المعلومات الشخصية الخاصة.

هناك بعض الخطوات التي تستطيع القيام بها لحماية نفسك وعائلتك من هذا الخطر:

1 تامين شبكة الواي فاي في منزلك:

الاجهزة الذكية تستعمل الانترنت لاستقبال وارسال معلومات , اذا كانت روابط الواي فاي غير امنه فان معلوماتك بالتالي غير امنه. اقل ما يمكن ان تفعله هو الحصول على تشفير لا سلكي وحماية لكلمة المرور.

تحت الاعدادات اللاسلكية تاكد بان جهاز التوجيه ممكن ال WPA2,

بعد ذلك اغلق شبكتك اللاسلكية بكلمة مرور قوية ومميزة عادة ما تكون بمزج احرف كبيرة مع احرف صغيرة مع ارقام مع رموز.

اذا كنت من المستعملين المتقدمين انشيء منطقة شبكة منفصلة على شبكة الواي فاي الخاصة بك لتوصل اجهزتك الذكية بها. هذا ما يسمى بعزل الجهاز ويعمل تماما كواي فاي الضيوف.

عندما تستعمل جهازك في الخارج اتصل بشبكات موثوقه ومزودة بكلمة مرور واعزل تطبيق ايجاد واي فاي اوتوماتيكيا.

2 قم بايقاف تشغيل تحديد الموقع الجغرافي اذا لم يكن قيد الاستخدام :

العديد من الاجهزة تحتوي على تطبيقات تمكنها من معرفة موقعك الجغرافي لتقديم بعض الخدمات كالخرائط او تتبع اللياقة البدنية , اذا كان هذا التطبيق قادر على تحديد موقعك فالقراصنة قادرون كذلك لذلك عندما لا تكون تستخدم هذه الخاصية اذهب الى الاعدادات واغلقها.

3 قبل تثبيت التطبيقات , تفهم سياسة خصوصية التطبيق وتعلميات الاستخدام :

تحتوي جميع التطبيقات على إعدادات خصوصية تساعد في التحكم في من يمكنه رؤية معلوماتك وماذا يمكنهم رؤيته. حدد هذه الاعدادات الخاصة والمعلومات الشخصية , مثل الاسم الكامل ومعلومات التواصل كذلك انتبه من التطبيقات التي تسأل اسئلة غير ضرورية او مفرطه , الق نظرة جيدة على الاذونات ولا تنقر فوق كلمة "سماح" على اي شيء.

4 . تعطيل الميكروفونات والكاميرات عندما لا تكون قيد الاستخدام:

تأتي معظم سماعات الألعاب وأجهزة التلفزيون الذكية والساعات الذكية ومكبرات الصوت الذكية مع ميكروفون و / أو الكاميرا. إن لم يكن آمنًا ، يمكن لجهازك إرسال المعلومات إليك لا تعقد النية على استعمالها. قم بإيقاف تشغيل الكاميرا ، وكتم صوت الميكروفون ، عندما لا تكون تستعملها.

5 انشىء اسم مستخدم لا يحتوي على معلومات تعريفية:

الافراط في المعلومات قد يعرض خصوصيتك للخطر , عند اعداد تسجيل الدخول لجهازك(او لعبة أو تطبيق) ، تأكد من أن اسم المستخدم لا يحتوي على معلومات تعريف ، مثل اسمك او عمرك او موقعك او معلومات الاتصال الخاصة بك

كن ذكيا في استعمال الهواتف الذكية

يمكن للهواتف الذكية تتبع موقعك والكشف عن معلومات عنك ، بما في ذلك موقعك معلومات الاتصال. احرص على تنزيل التطبيقات ذات السمعة الطيبة واستخدامها فقط ، وتأكد من كلمة المرور (أو بصمة) حماية هاتفك. معرفة كيفية استخدام الأدوات لإيجاد او محو الشخصية, البيانات من الهواتف المفقودة. ستجد المزيد على

ConnectSafely.org/cellphone-safety-tips.

تأمين مسار الإنترنت الخاص بك

من المحتمل وجود جهاز صغير في منزلك ، يسمى جهاز التوجيه أو مودم النطاق العريض الذي يوصلك بالإنترنت. يحتوي هذا الجهاز على كلمة مرور واسم مستخدم وأحيانًا يكون من السهل جدًا تخمين كلمات المرور الافتراضية. قد يصعب تكوين أجهزة التوجيه ، لذا إذا كنت في شك ، فاتصل بخبير أو بمزود خدمة الإنترنت لديك للحصول على المشورة بشأن كيفية تغيير كلمة المرور

حماية الأجهزة الخاصة بك

من خلال التأكد من أنها محمية بكلمة مرور ، وفي حالة أجهزة الكمبيوتر ، تأكد من وجود برنامج أمان وجدار حماية جيد. إذا كنت بحاجة إلى مساعدة ، فتواصل مع الأصدقاء أو العائلة ذوي المعرفة أو مزود خدمة الإنترنت أو مشغل الهاتف المحمول.

وبعض موفري خدمات الإنترنت الآخرين برنامجًا مجانيًا لمكافحة الفيروسات ، أو يمكنك Comcast تقدم شراء أو الحصول على برنامج أمان مجاني من شركة محترمة مثل تلك المدرجة في ConnectSafely.org/securityvendors.

موارد أخرى موصى بزيارتها لنصائح إضافية:

FightSpam.gc.ca:

ساعد الكنديين والشركات على تجنب البريد العشوائي والتهديدات الإلكترونية الأخرى

خصوصية الشباب: معلومات وأدوات من مكتب مفوض الخصوصية لمساعدة الشباب على حماية خصوصيتهم عبر الإنترنت.

التسوق عبر الإنترنت كيف تحمي نفسك عندما تتسوق عبر الانترنت:

استخدام كلمات المرور الفريدة والمتميزة: مرة أخرى ، كلمات المرور القوية ضرورية ،

كما هو الحال مع حسابات البريد الإلكتروني ووسائل التواصل الاجتماعي. لا تشارك أبدًا كلمات المرور الخاصة بك لأي شخص ، ما لم تقم بتعيين شخص تثق به لإدارة حساباتك. تأكد ان تحتوي كلمات مرورك على ثمانية أحرف على الأقل. تشمل الأرقام والأحرف الكبيرة والصغيرة والرموز ، ولا تستخدم أسماء أو كلمات القاموس. في

.ConnectSafely.org/passwords

ستجد نصائح ومعلومات حول كيفية استخدام المصادقة متعددة العوامل وبصمات الأصابع ومعلومات لمزيد .من الأمن المتقدم

لا تنقر على الروابط: في البريد الإلكتروني أو على وسائل التواصل الاجتماعي من البنوك وشركات بطاقات الائتمان ، الوكالات الحكومية أو المنظمات الأخرى ، ما لم تكن متأكدًا بنسبة 100٪ من أنها شرعية.

هناك عملية احتيال شائعة ، تسمى الخداع ، حيث يرسل إليك شخص ما رابطًا إلى ما يشبه

موقع شرعي ، ولكنه في الواقع موقع احتيال أنشأه مجرمون لسرقة معلومات تسجيل الدخول أو غيرها من

المعلومات الشخصية. حتى إذا كان اسم الشركة جزءًا من عنوان الويب ، فقد لا يزال

احتيال. رهانك الأكثر أمانًا هو كتابة عنوان الويب كما تفعل عادةً ، وإذا كنت في شك ، فاتصل بـ

المنظمة المعنية.

كن حذرًا من أي عرض يسعدك أن يكون صحيحًا: مثل إخبارك بانك قد فزت بمسابقة لم تدخلها , او يعرض عليك سعر لا يصدق لاجازة او ان ثمن المنتج اقل مما تتوقع دفعه . كن حذرًا بشكل خاص بشأن العروض منخفضة التكلفة, اسعار الادوية او التغطية الصحية.

تسوق فقط في متاجر أون لاين الشهيرة: كن حذرًا في أي موقع على الإنترنت, احذر التاجر الذي لم يسمع به من قبل. كثيرون شرعيون لكن البعض قد يسرق رقم بطاقتك الائتمانية أو غيرها من المعلومات المالية ، أو ببساطة تفشل في تقديم ما لديك مدفوع لأجل. عندما تكون في شك ، اطلب من شخص مطلع على التسوق عبر الإنترنت أو القيام ببعض الأبحاث عبر الإنترنت لمعرفة ما إذا كانت هناك ملاحظات أو تعليقات حول التاجر

عند التسوق او البحث عن البنوك لضمان موقع امن يجب ان يكون شريط المتصفح يبدا ب

https وجود حرف s يدل على انه موقع امن اما بدون وجود الحرف فهو موقع غير امن.

اذا كنت تتتسوق أو تتواصل مع البنك باستخدام تطبيق جوال ، تأكد من إصداره من قبل هذه الشركة, ابحث عن اراء الناس على الشبكة العنكبوتيه أو اسأل أحد الخبراء إذا كنت غير متأكد.

.

استخدم بطاقات الائتمان إذا كان ذلك ممكناً: وإلا ، استخدم بطاقات الخصم أو الدفع الآمن عبر الإنترنت

الخدمات ، مثل باي بال. لا ترسل أبدًا مبالغ نقدية أو شيكات أمين الصندوق أو حوالات مالية. حتى إرسال

الشيكات الشخصية يمكن أن تكون خطيرة. من الأفضل استخدام بطاقة ائتمان لأنه في حالة وجود نزاع ،

ستقوم شركة بطاقة الائتمان بإيقاف الرسوم أو استرداد أموالك أثناء التحقيق.

تتمتع بطاقات الخصم أيضًا بالحماية ، لكن عليك في بعض الأحيان الانتظار للحصول على أموالك

ببعض الخدمات مثل باي بال او اندرويد باي او ابل تتمتع بالحماية الا ان بطاقات الائتمان هي افضل وسيلة

كن حذرًا قبل النقر: هناك بعض الأشياء التي قد لا تكون قادرًا عليها

.التراجع ، مثل شراء أو بيع الأسهم الخطأ أو شراء رحلة غير قابلة للاسترداد أو غرفة فندق

راجع بعناية جميع المعاملات قبل تأكيدها. إذا قمت بخطأ ما اتصل بـ الشركة على الفور لمعرفة ما إذا كان من الممكن التراجع عنها. العديد من التجار عبر الإنترنت لديهم ميزة إلغاء تتيح لك التراجع عن عملية الشراء ، ولكن يجب عليك القيام بذلك على الفور.

بمجرد جهوزية السلعة للشحن قد يكون فات الأوان لإلغاء الطلب. يمكنك في كثير من الأحيان إرجاع مشترياتك ، لكن من المحتمل أن تضطر لدفع تكاليف إعادة الشحن.

تأكد من فهم سياسات الإرجاع من التجار عبر الإنترنت ومعرفة جميع الرسوم ، بما في ذلك الشحن ورسوم المناولة والضرائب.

قم ببعض الأبحاث قبل التبرع لأسباب عبر الإنترنت: مواقع التمويل الجماعي

هي أماكن رائعة لتكون من بين الداعمين الأوائل أو GoFundMe و Indiegogo و Kickstarter مثل

مشتري المنتجات الجديدة ، والتبرع لأسباب جديرة ، وحتى تقديم الدعم المالي للأشخاص الذين يعانون من حاجة ملحة ، ولكن يجب عليك المتابعة بحذر. اقرأ بعناية المطبوعة وقم بإجراء القليل من البحث عن الشخص أو المنظمة فاذا كانوا يجمعون المال لسبب ما ، حاولوا معرفة ما إذا كان هذا حقيقيًا ، وما إذا كانوا يطلقون خدمة جديدة رائعة. عندما تكون في شك لا تدخل رقم الضمان الاجتماعي الخاص بك على الإنترنت

إلا إذا كنت تعلم أنك في موقع شرعي لديه حاجة حقيقية لتلك المعلومات ، مثل

التقدم بطلب للحصول على حساب مصرفي أو بطاقة ائتمان أو قرض (من مؤسسة مالية شرعية) ، أو

الحصول على تقرير الائتمان. ما لم تكن متأكدًا من أنه موقع شرعي ، تجنب نشر معلوماتك بالكامل

تاريخ ومكان الميلاد ، وكن حذرًا عند مطالبتك بإدخال أي معلومات شخصية أخرى ،

مثل عنوان منزلك. مواقع وسائل الإعلام المشروعة مثل الفيسبوك والمؤسسات المالية قد

تكون هناك حاجة لطلب تاريخ ميلادك. فقط الكشف عن أرقام بطاقات الائتمان الشرعية عبر الإنترنت

بالنسبة للتجار. عندما تكون في شك ، قم ببعض الأبحاث لمعرفة ما يقوله الآخرون والمراجعون عنهم

مراقبة حساباتك المالية عبر الإنترنت: ابحث عن النشاط الأخير للتأكد

عدم وجود أي رسوم احتيالية على حسابك الائتماني أو المدين أو الحسابات المصرفية. تحقق على الانترنت الخاص بك

حسابات الاستثمار للتأكد من عدم وجود نشاط غير مصرح به. إذا وجدت

شيء مشبوه ، أبلغ عن ذلك على الفور إلى قسم الاحتيال في المؤسسة المالية أو

الرقم المجاني على بطاقة الائتمان أو الخصم الخاصة بك. حتى إذا كنت لا تستخدم خدمة الإنترنت ، فلا يزال هناك خطر ن تكون ضحية للاحتيال. أخبر المؤسسة على الفور إذا كانت هناك مشكلة. في

معظم الحالات تكون محميًا ضد الاحتيال ولكن يجب عليك الإبلاغ عنها

الاحتيال الخيري: لدى معظم المؤسسات الخيرية مواقع ويب وخيار للتبرع عبر الإنترنت. هذا جيد

.طالما كنت متأكدًا من أنك على الموقع الصحيح وأنها مؤسسة خيرية مشروعة تود دعمها

كن حذرًا إذا تلقيت رسالة بريد إلكتروني من مؤسسة خيرية على ما يبدو تطلب منك إنشاء اتصال عبر الإنترنت

CharityNavigator.org هبة. إذا لم تكن على دراية بالمنظمة ، فتحقق من ذلك على الموقع

ستتبرع عبر الإنترنت ، وكن على يقين من أنك ذاهب إلى موقع المؤسسة الخيرية. إلى

كن آمنا ، اكتب عنوان الويب الخيري في المستعرض بدلاً من النقر على الرابط

نصائح سريعة للتسوق عبر الإنترنت

(المصدر: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx)

بعض الدلائل تشير إلى أن موقع التسوق ليس جدير بالثقة

يبدو الموقع ضعيف التصميم وغير مهني ويحتوي على روابط مقطوعة

لا يمكنك العثور على عنوان أو رقم هاتف للعمل

يصعب العثور على سياسات المبيعات والعودة والخصوصية أو انها غير واضحة

الزر الخلفي معطل. وبعبارة أخرى ، تتعثر في صفحة و back لا استطيع العودة

يُطلب منك الحصول على معلومات بطاقة الائتمان في أي وقت بخلاف وقت وجودك

اتخاذ قرار الشراء

كيف تحمي نفسك عند التسوق عبر الإنترنت

الدفع عن طريق بطاقة الائتمان إذا كنت تستطيع. لا ترسل نقدا

كن على اطلاع على الأسعار التي تكون جيدة للغاية بحيث لا تكون حقيقية. انهم على الأرجح مزيفة

لا تستخدم شبكة عامة لغايات التسوق عبر الانترنت

اقرأ سياسة الخصوصية واكتشف كيف سيتم استخدام معلوماتك

لا ترد على رسالة بريد إلكتروني أو رسالة منبثقة تطلب فيها معلومات مالية

الشركات الشرعية لا تسأل عن المعلومات بطريقة غير مريحة

اقرأ بيانات بطاقة الائتمان الخاصة بك وتحقق من الرسوم غير المصرح بها statements

تأكد من تشغيل جدار الحماية الخاص بك.

لا تسمح بالملء التلقائي لكلمات المرور أو المعلومات الشخصية ، مثل كلمة المرور الخاصة بك

، وعدم السماح للموقع بتخزين معلومات بطاقة الائتمان الخاصة بك