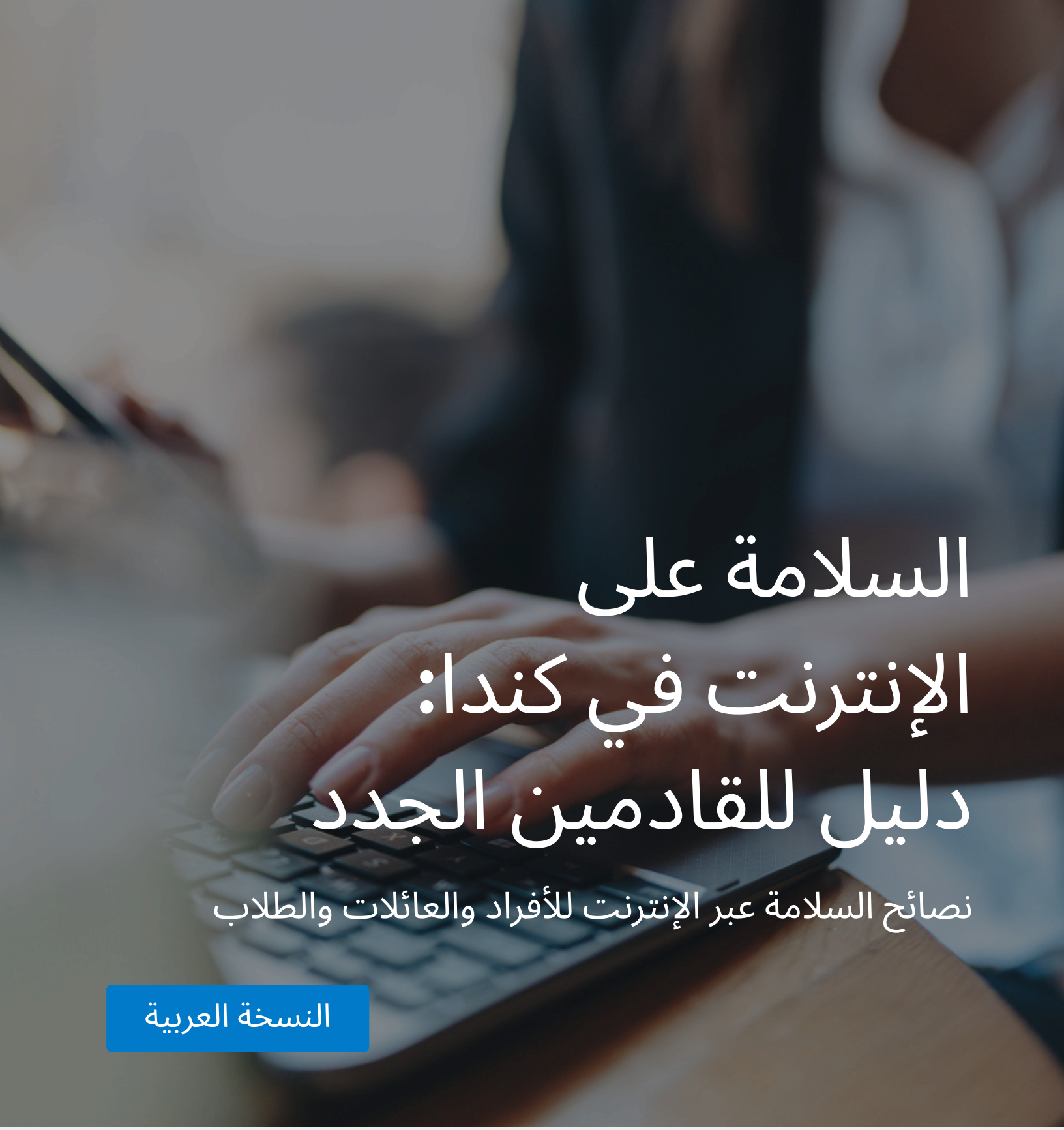


السلامة على الإنترنت في كندا: دليل للقادمين الجدد

نصائح السلامة عبر الإنترنت للأفراد والعائلات والطلاب

النسخة العربية

Settlement.Org
Welcome to Ontario

ROGERS

Toronto Metropolitan University

ROGERS cybersecure catalyst

المقدمة

الانتقال إلى بلد جديد يصاحبه العديد من التغييرات، ويمكن أن يكون الإنترنت أداةً رائعة لمساعدة القادمين الجدد على الاستقرار في كندا. إلا أن استخدام الإنترنت دون توخي الحذر قد يعرّضك للمخاطر.

تم إعداد هذا الدليل لمساعدتك على فهم المخاطر عبر الإنترنت، وستحصل من خلاله على نصائح عملية تساعدك على البقاء آمنًا عند استخدام الإنترنت، والتعرّف على الأمور التي يجب الانتباه لها، وكيفية حماية معلوماتك الشخصية، وما الذي ينبغي عليك فعله إذا كنت تعتقد أنك ضحية لعملية احتيال أو خداع عبر الإنترنت.

أعدّت Catalyst هذا الدليل بالشراكة مع OCASI - Ontario Council of Agencies Serving Immigrants وشركة Rogers، وذلك لمساعدة القادمين الجدد على البقاء آمنين عند استخدام الإنترنت.

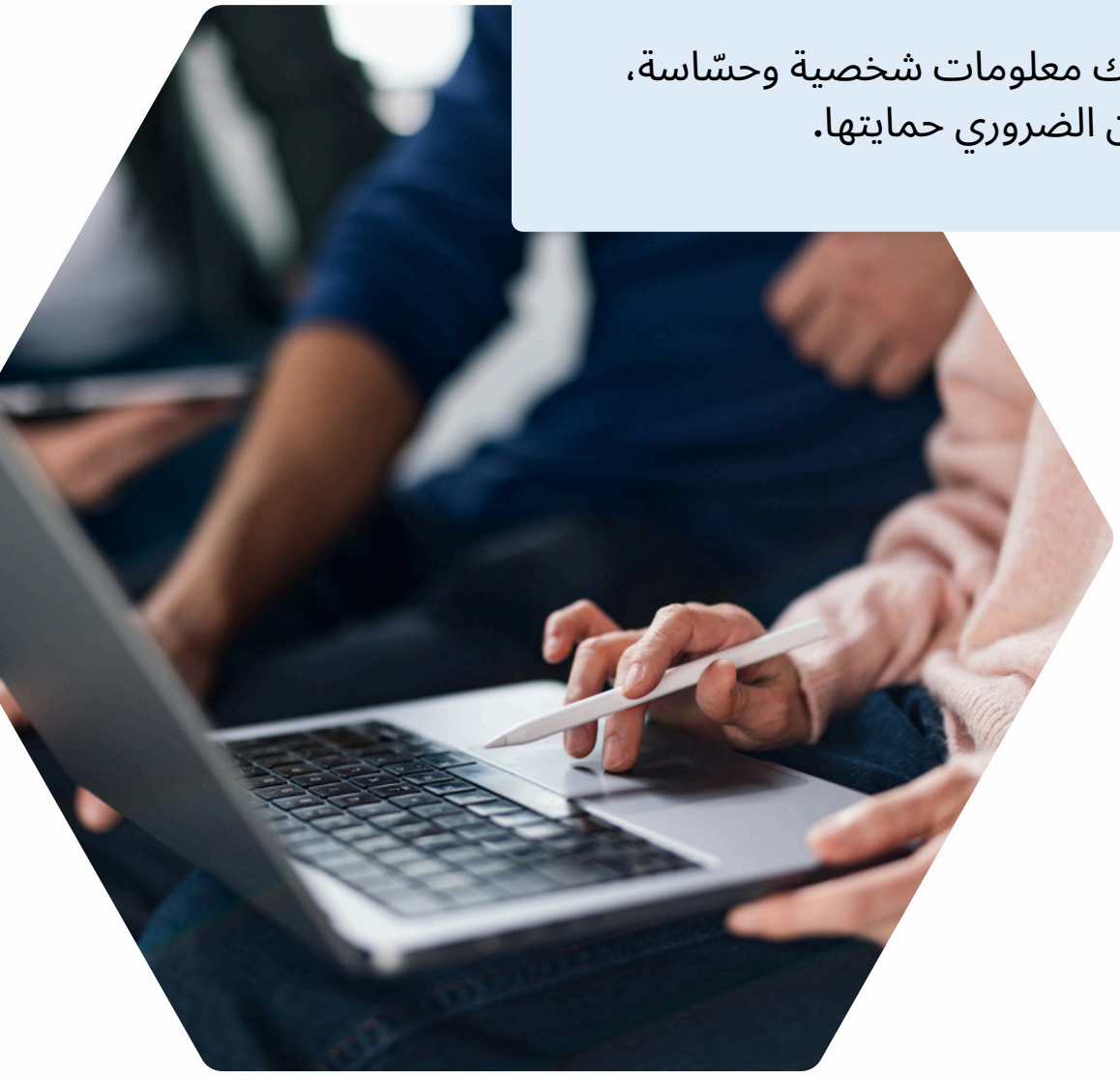
ما المخاطر التي ينبغي أن تكون على دراية بها عند استخدام الإنترنت؟

يُعدّ التواجد على الإنترنت جزءًا من الحياة اليومية الحديثة، ومن المهم فهم العوامل التي قد تعرّض معلوماتك الشخصية وسلامتك للخطر، مثل:

- الكشف عن بياناتك الشخصية والصحية
- إفشاء معلوماتك المالية أو إساءة استخدامها
- إساءة استخدام الصور التي تشاركها أو التلاعب بها
- التعرض للمضايقات والتحرّش

قد يحاول مجرمو الإنترنت أيضًا الاحتيال عليك أو استغلالك أو التنمّر عليك عبر الإنترنت.

لديك معلومات شخصية وحسّاسة، ومن الضروري حمايتها.



معرفة ما يمكن الوثوق به على الإنترنت

أفضل وسيلة لحماية نفسك من عمليات الاحتيال أو الخداع عبر الإنترنت هي التعرّف على الأنشطة المشبوهة، مثل المكالمات أو الرسائل الواردة من مصادر غير معروفة. قبل الضغط على أي رابط أو مشاركة أي معلومات، اسأل نفسك الأسئلة التالية:

- هل هذا أمر كنت تتوقعه؟
- هل تعرف المرسِل، وهل يبدو موثوقًا؟
- هل يطلب المرسِل معلومات شخصية أو معلومات حسّاسة أخرى؟
- هل يستخدم المرسِل الخوف أو التهديد أو الاستعجال أو الإكراه لدفعك إلى القيام بشيء ما أو للحصول على معلومات؟

هذه مجرد بعض المؤشرات التي تدل على ضرورة توخي الحذر. إن أخذ لحظة للتأكد والتحقق يمكن أن يساعدك على البقاء آمنًا.

إذا كنت غير متأكد، فلا تردّ.

طرق التحقق

- ابحث عن صفحة رسمية أو رقم هاتف من خلال مصدر آخر للتحقق مما إذا كان المرسِل موثوقًا به.
  - تمتلك بعض الجهات الحكومية، مثل وكالة الإيرادات الكندية، صفحات مخصصة للتحقق مما إذا كانت قد تواصلت معك بالفعل.

- إذا أُرسل إليك رابط أو مرفق، مرّر مؤشر الفأرة فوقه.
  - ملاحظة: تنجح هذه الطريقة على جهاز الكمبيوتر فقط وليس على الهاتف. هل يبدو عنوان الرابط أو الاسم منطقيًا؟ إذا كنت غير متأكد، فلا تضغط عليه — تحقق من خلال مصدر موثوق.

- احذر من المنتحلين الذين يتظاهرون بأنهم أحد أفراد عائلتك للحصول على معلومات منك.
  - فكّر في أن يتفق أفراد العائلة على «كلمة أمان» سرية مشتركة للمساعدة في التأكد مما إذا كان المتصل هو فعلًا أحدهم.

- الإجراء الأساسي هو التوقف والتحقق قبل الرد أو الاستمرار في أي تفاعل آخر.

كيفية البقاء أكثر أمانًا على الإنترنت

إلى جانب العادات الآمنة، يُعدّ استخدام الأدوات والإعدادات المناسبة جزءًا مهمًا من الحفاظ على الأمان عبر الإنترنت. فيما يلي بعض الخطوات التي يمكنك اتخاذها:

1. تأمين حساباتك:

- استخدم كلمات مرور قوية أو عبارات مرور.
- فعّل المصادقة متعددة العوامل (جهاز ثانوي، رمز، أو بيانات بيومترية).
- راجع إعدادات الخصوصية في حساباتك على وسائل التواصل الاجتماعي.
- اشترك مع البنك الذي تتعامل معه لتلقي تنبيهات بشأن الاحتيال.

2. تأمين اتصالاتك:

- أمّن شبكة Wi-Fi المنزلية بتغيير كلمة المرور الافتراضية إلى كلمة مرور قوية.
- أوقف تشغيل البلوتوث عندما لا يكون قيد الاستخدام.
- إذا احتجت إلى استخدام شبكة Wi-Fi عامة، فاحرص على ذلك عبر شبكة افتراضية خاصة (VPN).

3. تأمين أجهزتك:

- عيّن كلمات مرور قوية أو رموز وصول أو عبارات مرور أو أرقام تعريف شخصية (PINs) على جميع أجهزتك.
- ثبّت واستخدم برامج أمنية موثوقة على جميع الأجهزة.
- حافظ على تحديث البرامج واحذف التطبيقات والبرامج غير المستخدمة.
- احتفظ بالتحكم المادي بأجهزتك وتجنب مشاركتها مع أشخاص لا تعرفهم.
- أنشئ نسخًا احتياطية لبياناتك وبرامجك الأساسية.

للمزيد من المعلومات حول بعض الإجراءات التي توصي بها حكومة كندا للبقاء آمنًا على الإنترنت، يُرجى زيارة: www.getcybersafe.ca

كيفية التصرف إذا كنت تعتقد أنك ضحية احتيال عبر الإنترنت

إذا كنت تعتقد أنك وقعت ضحية لعملية احتيال أو خداع عبر الإنترنت أو لأي جريمة إلكترونية أخرى، فينبغي عليك القيام بما يلي:

1. اتخاذ احتياطات إضافية حسب الحالة، مثل تغيير كلمات المرور، وإجراء فحوصات أمنية، أو مراجعة كشوفاتك المالية لرصد أي معاملات غير معتادة.
2. التواصل مع البنك أو شركة بطاقة الائتمان الخاصة بك إذا كنت تعتقد أن حساباتك أو بطاقاتك الائتمانية قد تكون معرضة للخطر.
3. في الحالات الخطيرة، اتصل برقم الشرطة المحلي المخصص للحالات غير الطارئة.
4. الإبلاغ عن عمليات الاحتيال أو الخداع إلى المركز الكندي لمكافحة الاحتيال عبر الرابط التالي: https://antifraudcentre-centreantifraude.ca/index-eng.htm

أمثلة على الحوادث التي ينبغي الإبلاغ عنها للشرطة المحلية، والمؤسسات المالية، والمركز الكندي لمكافحة الاحتيال:

سرقة الهوية:
قام شخص ما بسرقة معلوماتك الشخصية واستخدامها لفتح بطاقات ائتمان أو الحصول على قروض باسمك. تواصل مع الشرطة المحلية والمؤسسات المالية التي تتعامل معها.

الاحتيال المالي:
عَلمت أو تشك في أنه قد تم سحب أموال غير مصرح بها من حسابك البنكي. تواصل مع الشرطة المحلية، والمؤسسات المالية، والمركز الكندي لمكافحة الاحتيال.

التصيّد الاحتيالي والهندسة الاجتماعية:
تم خداعك لمنح شخص ما إمكانية الوصول إلى حساباتك.

التحرّش عبر الإنترنت والتنمر الإلكتروني:
تلقيت رسائل تهديد أو تم نشر معلوماتك الخاصة على الإنترنت.

كيف يمكن للطلاب البقاء آمنين على الإنترنت

يُعدّ الطلاب من الفئات الأكثر استهدافًا من قبل مجرمي الإنترنت والمحتالين. غالبًا ما تستدرج العمليات الاحتيالية الطلاب بعروض سريعة مثل تحسين الدرجات، أو تقديم قروض طلابية منخفضة التكلفة، أو توفير أوراق امتحانات مجانية للمساعدة على النجاح. لكن إذا بدا العرض جيدًا لدرجة يصعب تصديقها، فهذه علامة على أنه قد يكون عملية احتيال.

رقمك الجامعي وسجلاتك ومعلوماتك المالية هي معلومات ذات قيمة كبيرة لمجرمي الإنترنت. لذلك، كن حذرًا عند مشاركتها مع أي شخص خارج مؤسستك التعليمية، وإذا كنت تعتقد أنه قد تم الكشف عن معلوماتك دون إذنك، فأبلِغ مكتب أمن المؤسسة التعليمية أو أي جهة رسمية أخرى – فمن المحتمل أنك لست الشخص الوحيد المتأثر بذلك.

مساعدة أفراد العائلة على البقاء آمنين على الإنترنت

قد يواجه الأطفال مخاطر جسيمة عبر الإنترنت، بما في ذلك التعرض للخداع أو الضغط من قبل غرباء، أو التنمّر الإلكتروني، أو الملاحقة، أو الطلب منهم مشاركة صور شخصية.

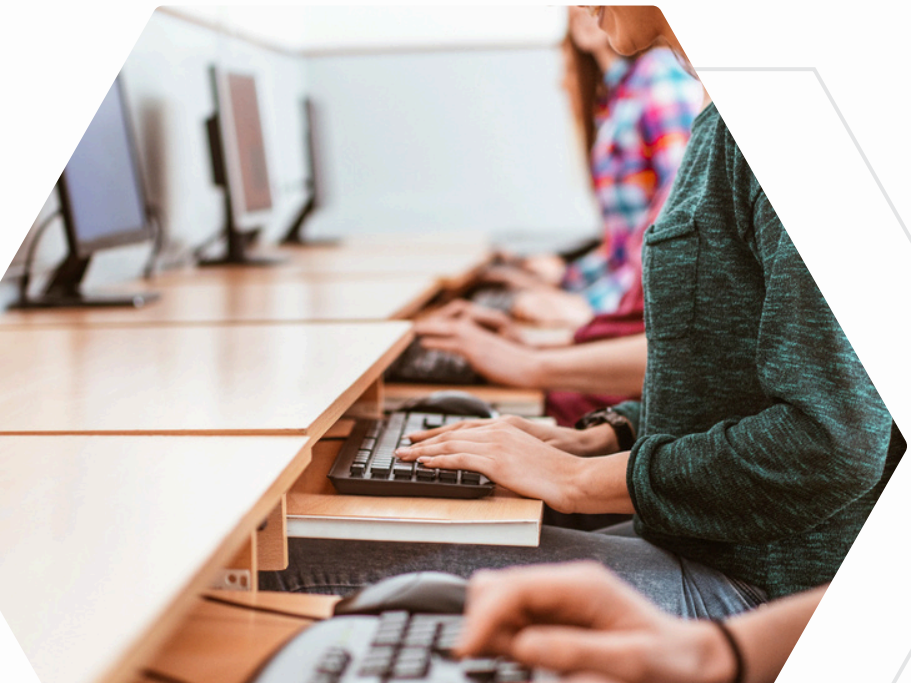
قد تكون هذه المواقف مزعجة ومؤذية، لذلك من المهم التحدث بصراحة مع طفلك حول كيفية البقاء آمنًا على الإنترنت. ذكّرهم بعدم مشاركة أي معلومات شخصية أو صور أو مقاطع فيديو مع أشخاص لا يعرفونهم، وبإبلاغك فورًا إذا صادفوا أي شيء عبر الإنترنت يجعلهم يشعرون بعدم الارتياح.

موارد إضافية

إلى بجانب مراجعة إعدادات الأمان الخاصة بطفلك على الإنترنت والإبلاغ عن التهديدات المشتبه بها إلى الجهات المسؤولة، ينبغي أيضًا النظر في الإبلاغ عن أي حوادث تتعلق بالاستغلال الإلكتروني للأطفال إلى موقع cybertip.ca.

إذا كان طفلك بحاجة إلى التحدث مع شخص آخر حول ما يمرّ به عبر الإنترنت، يمكنك تشجيعه على التواصل مع جهات الدعم المتاحة، مثل:

- Kids Help Phone — خدمة الصحة النفسية الإلكترونية الوحيدة في كندا المتاحة على مدار الساعة (24/7)، وتوفر دعمًا مجانيًا وسريًا ومتعدد اللغات. يمكن إرسال كلمة CONNECT إلى الرقم 686868 أو زيارة الموقع: kidshelpphone.ca.
- Good2Talk — خدمة دعم مجانية وسرية لطلاب ما بعد المرحلة الثانوية في أونتاريو ونوفا سكوشا، ومتاحة بأكثر من 100 لغة. يُرجى زيارة: Good2Talk.ca.



الخلاصة

يوفّر الإنترنت العديد من الفوائد، إلا أن مجرمي الإنترنت يبحثون دائمًا عن فرص لاستغلال الأشخاص عبر الإنترنت. لديك القدرة على حماية نفسك وأحبّائك من خلال طرح الأسئلة واتباع عادات استخدام آمنة للإنترنت.

يقدّم هذا الدليل أمثلة ونصائح لمساعدتك على البقاء آمنًا ومحصّنًا عند استخدام الإنترنت. لمزيد من الموارد، يُرجى زيارة الأدلة الإلكترونية المخصّصة للقادمين الجدد والعائلات والطلاب.

اطّلع على مزيد من المصادر

cybersecurecatalyst.ca/cyber-resources-for-educators-schools

مصطلحات يجب معرفتها

فيما يلي بعض الكلمات والعبارات الشائعة المستخدمة في هذا الدليل. يقدّم هذا المسرد تعريفات قصيرة وواضحة لمساعدتك على المتابعة والبقاء آمنًا عند استخدام الإنترنت:

الاحتيال:
عرض أو رسالة مزيفة صُمِّمت لخداعك ودفعك إلى تقديم شيء ذي قيمة، مثل المال أو المعلومات الشخصية.

التهديدات:
عندما يقول أو يفعل شخص ما شيئًا يجعلك تشعر بعدم الأمان، وغالبًا ما يكون ذلك بهدف إخافتك للقيام بما يريده بالإكراه.

الإكراه أو الضغط:
عندما يضغط عليك شخص ما أو يجبرك على القيام بشيء لا ترغب في فعله.

عنوان URL (مُحدِّد موقع الموارد الموحد):
الرابط الإلكتروني الذي تكتبه في المتصفح لزيارة موقع إلكتروني. على سبيل المثال: getcybersafe.ca.

المنتحلون:
أشخاص يتظاهرون بأنهم شخص آخر (مثل صديق، أو أحد أفراد العائلة، أو شركة) لكسب ثقتك.

كلمة الأمان:
كلمة أو عبارة سرية تتفق أنت وشخص تثق به على استخدامها، حتى تتمكن من التأكد من أنه هو بالفعل.

المصادقة متعددة العوامل:
إجراء أمني يتطلب أكثر من مجرد كلمة مرور، مثل رمز يُرسل إلى هاتفك أو التحقق باستخدام بصمة الإصبع.

البلوتوث:
تقنية لاسلكية تتيح للأجهزة (مثل سماعات الرأس أو مكبرات الصوت) الاتصال ببعضها البعض دون استخدام الكابلات.

عبارة المرور:
نوع من كلمات المرور تتكوّن من عدة كلمات أو أرقام أو رموز مجتمعة، مما تجعل معرفتها أكثر صعوبة.
مثال: Newcomer$afety!Guide2025

الرقم التعريفي الشخصي (PIN):
رمز رقمي قصير، غالبًا ما يتكوّن من 4 إلى 6 أرقام، يُستخدم لفتح الحسابات أو الأجهزة (مثل الهاتف).

برامج الحماية الأمنية:
برامج أو تطبيقات يتم تثبيتها على الأجهزة للمساعدة في حمايتك من الفيروسات والبرمجيات الخبيثة.

التصيّد الاحتيالي والهندسة الاجتماعية:
أساليب يستخدمها المجرمون لمحاولة خداعك ودفعك إلى الإفصاح عن معلوماتك الشخصية، وغالبًا ما تتم عبر مكالمات هاتفية، أو رسائل بريد إلكتروني مزيفة، أو رسائل نصية، أو مواقع إلكترونية وهمية.

التنمّر الإلكتروني:
عندما يستخدم شخص ما الإنترنت للتحرّش أو التهديد أو إحراج شخص آخر.

كلمة المرور القوية:
كلمة مرور طويلة وفريدة، تستخدم مزيجًا من الحروف والأرقام والرموز، وتتجنب المعلومات الشخصية، مما يجعل تخمينها أو اختراقها أمرًا صعبًا.

المعلومات الشخصية:
أي معلومات تُعرّف بك، مثل اسمك أو عنوانك أو رقم هاتفك أو مؤسستك التعليمية، يمكن لمجرمي الإنترنت استخدامها لسرقة هويتك أو ارتكاب عمليات احتيال.

المعلومات الصحية:
تشمل المعلومات الصحية تاريخك الطبي، وزيارات الطبيب، أو تفاصيل التأمين الصحي، وهي معلومات خاصة وذات قيمة لمجرمي الإنترنت الذين قد يستغلونها في عمليات احتيال.

الأمن السيبراني للجميع

تواصل معنا

cybersecurecatalyst.ca