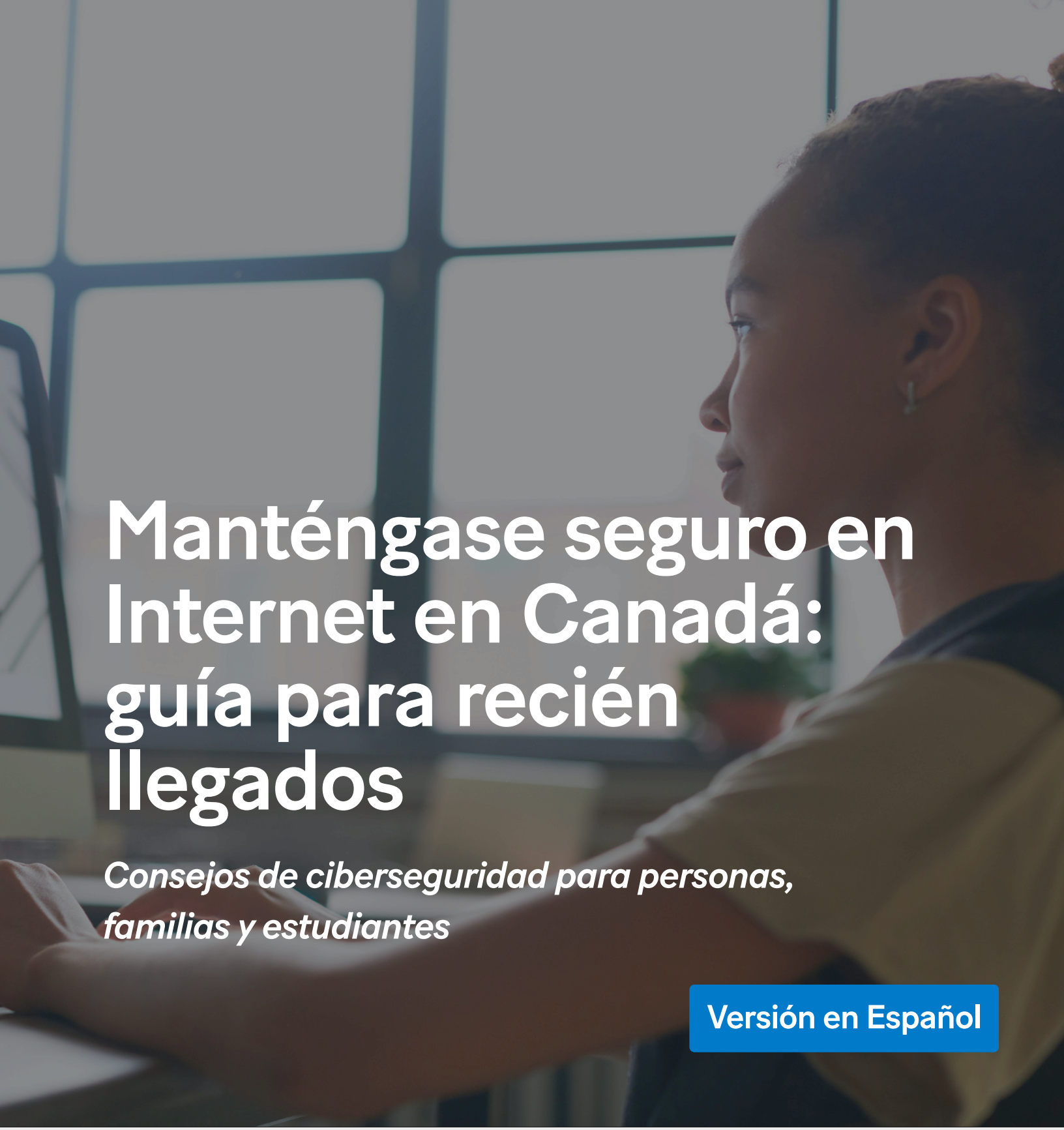

Manténgase seguro en Internet en Canadá: guía para recién llegados

Consejos de ciberseguridad para personas, familias y estudiantes

Versión en Español

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

Settlement.Org Welcome to Ontario

Introducción

Mudarse a un nuevo país conlleva muchos cambios, y el Internet puede ser una gran herramienta para ayudar a los recién llegados a establecerse en Canadá. Pero navegar por este proceso sin precaución también puede exponerlo a riesgos en línea.

Esta guía está diseñada para ayudarlo a comprender los riesgos en línea. Obtendrá consejos prácticos que le ayudarán a mantenerse seguro al utilizar Internet, aprenderá a qué debe prestar atención, cómo proteger su información personal y qué hacer si cree que ha sido víctima de una estafa o fraude en línea.

The Catalyst ha elaborado esta guía en colaboración con OCASI - Ontario Council of Agencies Serving Immigrants y Rogers para ayudar a los recién llegados a mantenerse seguros en Internet.

¿Qué riesgos hay que tener en cuenta en Internet?

Estar conectado a Internet forma parte de la vida cotidiana moderna, y es importante comprender qué factores pueden poner en riesgo su información personal y su seguridad, tales como:

- La divulgación de sus datos personales y médicos
- La divulgación o el uso indebido de su información financiera
- El uso indebido o la manipulación de las imágenes que comparte
- El acoso

Los ciberdelincuentes también pueden intentar estafarlo, explotarlo o intimidarlo en línea.

Usted tiene información personal y sensible, y es fundamental protegerla.

Saber en qué se puede confiar en Internet

La mejor manera de protegerse de las estafas o fraudes en Internet es reconocer las actividades sospechosas, como las llamadas o mensajes de fuentes desconocidas. Antes de hacer clic en un enlace o compartir información, hágase estas preguntas:

- ¿Es algo que espera?
- ¿Conoce al remitente y le parece legítimo?
- ¿Solicitan información personal u otra información sensible?
- ¿Están utilizando el miedo, las amenazas, la urgencia o la coacción para conseguir que haga algo o para obtener información?

Estos son solo algunos de los indicadores que sugieren que debe ser cauteloso. Tomarse un momento para verificar dos veces puede ayudarlo a mantenerse seguro.

Si no está seguro, no responda.

Formas de verificar

- Busque una página oficial o un número de teléfono a través de otra fuente para verificar si el remitente es legítimo.
  - Algunos organismos públicos, como la Agencia Canadiense de Ingresos (Canada Revenue Agency o CRA, por sus siglas en inglés), tienen páginas web dedicadas a verificar si le han llamado o no.
- Si le envían un enlace o un archivo adjunto, pase el cursor por encima.
  - Nota: esto solo funciona en una computadora, no en un teléfono. ¿Tiene sentido la URL o el nombre? Si no está seguro, no haga clic: consulte con una fuente confiable.
- Tenga cuidado con los suplantadores que se hacen pasar por su familia para sacarle información.
  - Considere la posibilidad de que los miembros de su familia memoricen una "palabra de seguridad" secreta y compartida para ayudarlos a identificar si realmente son ellos.
- La acción clave es HACER UNA PAUSA y VERIFICAR antes de responder o seguir adelante.

Cómo estar más seguro en Internet

Más allá de los hábitos seguros, el uso de las herramientas y configuraciones adecuadas es una parte importante de la seguridad en Internet. Aquí tiene algunas medidas que puede tomar:

1. Proteja sus cuentas:

- Use contraseñas o frases de contraseña seguras.
- Habilite la autenticación multifactor (un dispositivo secundario, un código o una autenticación biométrica).
- Revise la configuración de privacidad de sus redes sociales.
- Inscríbase en su banco o institución financiera para recibir alertas de fraude.

2. Proteja sus conexiones:

- Proteja la red Wi-Fi de su hogar cambiando la contraseña predeterminada por una contraseña segura.
- Desactive el Bluetooth cuando no lo utilice.
- Si necesita utilizar una red Wi-Fi pública, hágalo a través de una red privada virtual (VPN).

3. Proteja sus dispositivos:

- Establezca contraseñas, códigos de acceso, frases de contraseña o números de identificación personal (PIN) seguros en todos sus dispositivos.
- Instale y utilice software de seguridad confiable en todos los dispositivos.
- Mantenga actualizado el software y elimine las aplicaciones y el software que no utilice.
- Mantenga el control físico de sus dispositivos y evite compartirlos con personas que no conozca.
- Haga una copia de seguridad de sus datos críticos y de su software.

Visite www.getcybersafe.ca para obtener más información sobre algunas de las medidas recomendadas por el Gobierno de Canadá que puede adoptar para mantenerse seguro en Internet.

Cómo responder si cree que ha sido víctima de un fraude en línea

Si cree que ha sido víctima de una estafa, o un fraude en línea o otro delito cibernético, debe hacer lo siguiente:

1. Tomar precauciones adicionales según la situación, como cambiar sus contraseñas, realizar análisis de seguridad o comprobar sus estados financieros en busca de transacciones inusuales.
2. Contactar a su banco o institución financiera o a la compañía de tarjetas de crédito si cree que sus cuentas o tarjetas pueden estar en peligro.
3. Para incidentes graves, llame al número de no emergencias de la policía local.
4. Denunciar los fraudes o estafas al Centro de Lucha contra el Fraude de Canadá (Canadian Anti-Fraud Centre): https://antifraudcentre-centreantifraude.ca/index-eng.htm

Ejemplos de incidentes que debe comunicar a la policía local, a las instituciones financieras y al Centro de Lucha contra el Fraude de Canadá:

Robo de identidad:
alguien ha robado su información personal y la ha utilizado para obtener tarjetas de crédito o pedir préstamos a su nombre. Póngase en contacto con la policía local y con sus instituciones financieras.

Fraude financiero:
usted sabe o sospecha que se ha robado dinero sin autorización de su cuenta bancaria. Póngase en contacto con la policía local, sus instituciones financieras y el Centro de Lucha contra el Fraude de Canadá.

Phishing e ingeniería social:
lo han engañado para que le dé acceso a sus cuentas a alguien.

Acoso en línea y ciberacoso:
ha recibido mensajes amenazantes o han publicado su información privada en Internet.

Cómo pueden protegerse los estudiantes en Internet

Los estudiantes son el principal objetivo de ciberdelincuentes y estafadores. Estas estafas atraen a los estudiantes con ofertas rápidas para mejorar sus calificaciones, préstamos estudiantiles a bajo costo o exámenes gratuitos que los ayudarán a tener éxito. Pero si una oferta parece demasiado buena para ser cierta, es señal de que podría tratarse de una estafa.

Tu número de estudiante, expedientes e información financiera también son valiosos para los ciberdelincuentes. Ten cuidado a la hora de compartir esta información con personas ajenas a tu centro educativo. Si crees que tu información ha sido divulgada sin tu autorización, comunícalo a la Oficina de Seguridad o autoridad de tu centro educativo; es probable que no seas el único afectado.

Ayudar a los miembros de la familia a estar seguros en Internet

Los niños pueden correr graves riesgos en Internet, como ser engañados o presionados por desconocidos, sufrir ciberacoso, ser acosados o que se les pida que compartan imágenes personales.

Estas situaciones pueden ser perturbadoras y perjudiciales, por lo que es importante hablar abiertamente con su hijo sobre cómo mantenerse seguro en Internet. Recuérdele que no comparta información personal, fotos o videos con personas que no conoce y que le diga si algo que encuentra en Internet le hace sentir incómodo.

Recursos adicionales

Además de revisar la configuración de seguridad en línea de su hijo y reportar posibles amenazas a las autoridades policiales, también debería considerar denunciar cualquier incidente relacionado con la explotación infantil en línea a cybertip.ca.

Si su hijo necesita hablar con alguien sobre lo que está viviendo en Internet, puede animarle a ponerse en contacto con recursos que pueden ayudarle.

- Kids Help Phone: el único servicio de salud mental en línea de Canadá disponible las 24 horas del día, los 7 días de la semana, que ofrece asistencia gratuita, multilingüe y confidencial. Envíe un mensaje de texto con la palabra CONNECT al 686868 o visite kidshelpphone.ca.

- Good2Talk: un servicio de apoyo gratuito y confidencial para estudiantes de educación superior en Ontario y Nueva Escocia, disponible en más de 100 idiomas. Visite Good2Talk.ca.

Conclusión

Internet ofrece muchas ventajas, pero los ciberdelincuentes siempre buscan oportunidades para aprovecharse de la gente en línea. Usted tiene el poder de protegerse a sí mismo y a sus seres queridos haciendo preguntas y practicando hábitos de seguridad en Internet.

En esta guía encontrará ejemplos y consejos que le ayudarán a mantenerse seguro en Internet. Para obtener más recursos, visite nuestras guías en línea para recién llegados, estudiantes y familias.

Acceda a más recursos
cybersecurecatalyst.ca/cyber-resources-for-educators-schools

Términos que debe conocer

A continuación, se incluyen algunas palabras y frases comunes utilizadas en esta guía. Este glosario ofrece definiciones breves y claras para ayudarlo a seguir el contenido y mantenerse seguro en Internet:

Estafa:
una oferta o mensaje falso diseñado para engañarlo y conseguir que entregue algo valioso, como dinero o información personal.

Amenazas:
cuando alguien dice o hace algo que lo hace sentir inseguro, a menudo lo hace para asustarlo y que haga lo que desea.

Coacción:
cuando alguien lo presiona o lo obliga a hacer algo que no quiere.

URL (Localizador uniforme de recursos):
la dirección web que se teclea en un navegador para visitar un sitio web. Por ejemplo: getcybersafe.ca

Suplantadores:
personas que se hacen pasar por otras (como un amigo, un familiar o una empresa) para ganarse su confianza.

Palabra segura:
una palabra o frase secreta que usted y una persona de su confianza acuerdan utilizar para que pueda confirmar que realmente se trata de ella.

Autenticación multifactor (MFA):
una medida de seguridad que le solicita algo más que una contraseña, como un código enviado a su teléfono o un escaneo de huella digital.

Bluetooth:
tecnología inalámbrica que permite conectar dispositivos (como auriculares o altavoces) sin cables.

Frase de contraseña:
tipo de contraseña compuesta por varias palabras, números o símbolos combinados, lo que dificulta su adivinación.
Ejemplo: Guía$eguridad!reciénllegados2025

PIN (Número de identificación personal):
código numérico corto, a menudo de 4 a 6 dígitos, que se utiliza para desbloquear cuentas o dispositivos (como un teléfono).

Software de seguridad:
software o aplicaciones instaladas en dispositivos que ayudan a protegerlo de virus y software malicioso.

Phishing e ingeniería social:
tácticas utilizadas por los delincuentes para intentar engañarlo y que facilite información personal, a menudo a través de llamadas telefónicas, correos electrónicos falsos, mensajes de texto o sitios web.

Ciberacoso:
cuando alguien utiliza Internet para acosar, amenazar o avergonzar a otra persona.

Contraseña segura:
una contraseña segura es larga y única, y utiliza una combinación de letras, números y símbolos. Evita los detalles personales para que resulte difícil de adivinar o descifrar.

Información personal:
la información personal es cualquier detalle que lo identifique, como su nombre, dirección, número de teléfono o centro educativo. Los ciberdelincuentes pueden utilizarla para robar su identidad o cometer un fraude.

Información sobre la salud:
la información sobre la salud incluye su historial médico, visitas al médico o datos del seguro. Es privada y valiosa para los ciberdelincuentes, quienes podrían utilizarla para cometer fraudes.

Ciberseguridad para todos

Visítenos en

cybersecurecatalyst.ca

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

Settlement.Org Welcome to Ontario