BIPT

BURNABY
INTERCULTURAL
PLANNING TABLE

Estafas. Fraudee, Seguridad en Internet y Acoso en Línea

Consejos para Jóvenes, Padres y Adultos Mayores

Funded by:

Immigration, Refugees and Citizenship Canada

Finance par :

Immigration, Refugies et Citoyennete Canada

Estafas. Fraudee, Seguridad en Internet y Acoso en Línea

Consejos para Jóvenes, Padres y Adultos Mayores

TABLA DE CONTENIDO

Agradecimientos

Intercultural Connections Working Group

Andisheh Fard - SFU
Cindy Chang – City of Burnaby Recreation & Cultural Services
Darae Lee - MOSAIC
Deborah Baker – Squamish Nation
Duncan Olenick – Burnaby Public Library
Evelyn McGowan – Purpose Society / Burnaby Youth Hub
Gabriella Maio – Ministry of Children and Families Development
Heather McCain – Citizens for Accessible Neighbourhoods
Kimberly Barwich – Burnaby Neighbourhood House
Melody Monro – Fraser Health
Natalya Khan – Burnaby School District #41
Rebekah Mahaffey – City of Burnaby
Sangeeta Bhonsale – Burnaby Family Life
Shae Wiswanathan – SUCCESS
Tarana Sultan – PIRS
Thea Fiddick – ISS of BC

Traductores:

Arabe:	Abeer Hattab
Chino:	Derek Chen
	Tom Su
Persa:	Sossan Kayoumi
	Nabila Akbari
	Zarif Akbarian
Koreano:	Darae Lee
Español:	Mary Blanca Battenberg
	Pilar Sain
Tigriña:	Tigist Dubus Tesfamariam
	Daniel Debesay Michael
	Tedros Gebrengus
	Enbakom Berhane
	Asmait Tekle

Consejos de Seguridad en Internet Para Padres

Hable acerca de la seguridad en Internet: Existen peligros en Internet, desde preocuparse por la privacidad hasta el robo de identidad. Los niños y adolescentes necesitan supervisión cuando usan Internet, así tengan 5 o 15 años, los adultos deben mantenerse atentos. La atención sobre su seguridad, como compartir donde su localización, fotos e información personal,servira en gran medida para proteger a sus seres queridos.

- Cómo Estructurar la Tarea y el Tiempo en Línea: https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- 10 Consejos de Seguridad de Internet y Uso de Tecnología para Padres: https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- Consejos de Seguridad en Internet: Consejos Principales para Padres: https://www.webwise.ie/parents/advice-top-10-tips-for-parents/

Uso no supervisado / Uso Temprano de Internet: En una encuesta realizada por Shared Hope International, uno de cada ocho padres permite que sus hijos usen Internet desde los dos años y solo uno de cada 10 permite que sus hijos usen Internet cuando tienen 10 años o más, (como lo recomiendan los expertos). Como resultado, muchos niños usan Internet a temprana edad sin supervision. Aquí le indicamos cómo proteger a sus hijos mientras está en línea:

- https://protectkidsonline.ca/app/en/interests_and_risks-5_to_7
- https://protectkidsonline.ca/app/en/interests_and_risks-8_to_10
- https://protectkidsonline.ca/app/en/interests_and_risks-11_to_12
- https://protectkidsonline.ca/app/en/interests_and_risks-13_to_15

Monitoreando las Actividades en Línea de sus Hijos: desafortunadamente, independientemente de la participación de los padres, muchos adolescentes ocultan o eliminan su historial de navegación de sus padres. Es imperativo que los padres sean diligentes. Los adolescentes también tienen cuentas de correo electrónico o redes sociales que sus padres quizás desconocen. En algunos casos, los niños mienten sobre su edad para crear estas cuentas.

- https://protectkidsonline.ca/app/en/info_monitoring_online_activitie
- Como apoyo a los padres en casos en que los niños experimentan la victimización de sus compañeros, los padres deben consultar el recurso "Pirámide de Apoyo" en: https://witsprogram.ca/pdfs/families/pyramid-of-support.pdf

Teléfonos celulares: los teléfonos celulares son excelentes para mantenerse en contacto y en caso de emergencias. Aproximadamente el 69 por ciento de los niños de 11 a 14 años tienen sus teléfonos celulares. Los usuarios de teléfonos celulares deben comprender y ser conscientes de que el GPS de un teléfono celular puede revelar la ubicación física exacta del usuario. Además, siempre debe tener cuidado al publicar números de teléfonos celulares personales en línea.

- Cuándo Darle un Teléfono a su Hijo: https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- Consejos de Seguridad para Teléfonos Celulares: https://protectkidsonline.ca/app/en/info_phone_safety
- El Primer Teléfono Celular: Reglas de Responsabilidad: https://www.ahaparenting.com/Ages-stages/tweens/Cell-Phone-Rules-Safe-Responsible-Kids
- Aplicación de Monitoreo Parental para Rastrear teléfonos celulares en Canadá y más allá de las

Hablando sobre Seguridad en Internet con sus Hijos

Intimidación en línea: hay varias aplicaciones de conversaciones anónimas y sitios web donde se puede publicar

preguntas o información sobre otros (de forma anónima). Estas aplicaciones anónimas, que incluyen Whisper, Yik Yak y Ask.FM, son peligrosas porque se sabe que promueven el acoso (bullying) escolar. Ocultando sus identidades anónimas, los acosadores se burlan fácilmente y menosprecian a los demás. Es importante permanecer siempre diligente y reportar cualquier abuso, ya sea sospechoso o comprobado.

- PREVNet: la Red de Promoción de Relaciones y Eliminación de la Violencia es la autoridad de Canadá en investigación y recursos para la prevención del acoso escolar.
- ¿Qué hacer si su hijo está siendo intimidado ?: https://needhelpnow.ca/app/en/resources_cyberbullying
- Programa WITS: Los programas WITS reúnen a escuelas, familias y comunidades para crear entornos de apoyo a los niños a lidiar con el acoso escolar y la victimización de sus compañeros.
- RCMP Centre for Youth Crime Prevention: Centro de RCMP para la prevención del delito juvenil: proporciona a los canadienses información y herramientas para prevenir delitos juveniles y su victimización.
- Kids Help Line Línea de ayuda para niños, es un buen recurso para los padres y sus hijos. Proporciona acceso a asesoramiento ¿Necesita ayuda en este momento? Envía un mensaje de texto CONNECT al 686868 para chatear con un voluntario de respuesta a crisis 24/7. https://kidshelpphone.ca/search/?keys=Cyberbullying

Fotos Explícitas: la investigación indica que uno de cada siete adolescentes se ha tomado una fotografía desnuda(o) o semidesnuda (o) y más de la mitad de esas fotografías fueron compartidas con otra persona a través de Internet. Es importante tener en cuenta que una vez que la información se publica en Internet, muy posiblemente no hay forma de removerla por completo.

- Cybertip.ca: Linea canadiense de consejos para informar sobre la explotación sexual en línea de niños.
- https://protectkidsonline.ca/app/en/info_self_peer_exploitation
- https://protectkidsonline.ca/app/en/info_online_extortion
- https://protectkidsonline.ca/app/en/info_online_luring

Compras en línea, robo de identidad, navegación por la Línea (web): es importante ser cuidadoso al navegar en linea. Su historia de actividad es rastreada constantemente. Visitar sitios en linea inseguros o inapropiados puede comprometer su información personal y financiera o dañar su computadora. Es importante tener seguridad adecuada y un programa antivirus instalado.. Siempre use una conexión segura, Evite usar una computadora pública para garantizar que los sitios sean legítimos y seguros antes de realizar pedidos en línea. El uso de precauciones proporcionará una experiencia más segura. Los niños son víctimas de robo de identidad la mayoría de las veces. De hecho, en comparación con los adultos, los menores de 18 años tienen 51 veces más probabilidades que les roben su identidad. Los delincuentes atacan a los niños porque tienen registros de crédito limpios y con frecuencia publican información personal en línea.

- **Cómo encontrar el estado de crédito de un niño**, instrucciones paso a paso sobre cómo verificar el informe de crédito de su hijo: https://www.creditcards.com/credit-card-news/instructions-how-to-check-child- credit-report.php

Videojuegos: los videojuegos han recorrido un largo camino en los últimos años. Con muchas opciones de juego disponibles, los padres deben ser conscientes que la mayoría de los dispositivos de juego pueden conectar directamente a los niños aconInternet y otros jugadores. Afortunadamente, la mayoría de los dispositivos de juego tienen controles para padres y configuraciones de seguridad. Los padres deben limitar el tiempo con los videojuegos.

- Juegos educativos en línea recomendados para enseñar a niños y adolescentes en los grados 4 a 8 acerca de cómo estar seguros cuando usan Internet: http://mediasmarts.ca/digital-media-

literacy/educational-games

HABLANDO SOBRE LA SEGURIDAD EN INTERNET CON SUS HIJOS

FUENTE: http://www.family.ca/internet-safety-tips/

1. Mantenga su información personal en privado: no proporcione su nombre, número de teléfono, escuela o dirección sin el permiso de un padre / tutor.

2. La mayoría de los sitios de redes sociales como Facebook y Twitter le permitirán elegir quién puede ver sus publicaciones. Pídale a un adulto que lo ayude a cambiar su configuración de privacidad.

3. Tenga en cuenta que cualquier cosa que comparta en las redes sociales, incluso en privado, podría ser vista por otra persona. ¡Piense siempre dos veces antes de hacer clic en "publicar" o "enviar"!

4. Si ve algo inapropiado en línea, pida consejo a padres o adultos de confianza. Recuerda, ¡no es tu culpa que hayas visto esto!

5. Si alguien le envía algo grosero por correo electrónico o redes sociales, NO RESPONDA; en cambio, hable con un adulto responsable o de confianza.

6. Si está compartiendo fotos o videos que tienen otras personas en ellos, siempre solicite permiso primero.

7. Nunca compre algo en línea ni descargue nada sin el permiso de un padre o tutor.

8. Nunca acepte reunirse en persona con alguien que solo conoce en línea. ¡Recuerde que las personas pueden no ser quienes dicen ser!

9. ¡Mantenga sus contraseñas SECRETAS! ¡Ni siquiera sus mejores amigos necesitan saberlo!

10. Pongase de pie contra el acoso escolar: ¡no acepte chismes, ni humille a nadie! Si desea obtener más información sobre el acoso cibernético o el

Consejos para Adultos: Estafas, Fraudes y Seguridad Cibernética

LLAMADAS FRAUDULENTAS:

Tenga cuidado con las personas que llaman que afirman falsamente representar a una empresa u organización de confianza. https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdlnt-clls-en.aspx

QUÉ HACER SI RECIBE UNA LLAMADA:

Si recibe una llamada, cuelgue. Nunca le dé acceso remoto a su computadora en respuesta a una llamada no solicitada. Si no está seguro, comuníquese con el centro de servicio al cliente de la empresa u organización. Recomendamos encarecidamente a los canadienses que denuncien tales casos de fraude al Centro Canadiense contra el Fraude en: http://www.antifraudcentre-centreantifraude.ca o llamando al 1-888-495-8501.

ESTAFAS Y FRAUDES EN LINEA:

No siempre es fácil determinar si un correo electrónico, concurso o promoción es real o una estafa o fraude en Internet. Las ofertas pueden parecer demasiado buenas para ser verdad, y pueden serlo. La clave para estar seguro es reconocer los signos de los estafadores.
https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx

¿DÓNDE PUEDO OBTENER MÁS INFORMACIÓN ?:

Existen muchas buenas fuentes de información en línea sobre fraude y estafas. El sitio de internet de la Agencia del Consumidor Financiero de Canadá proporciona información sobre sus derechos al tratar con bancos y otras instituciones financieras.

Para pedir copias adicionales de esta publicación, o para obtener ayuda para encontrar un número de teléfono en nuestra provincia o territorio, llame al 1 800 O-Canada (1-800-622-6232), TTY: 1-800-926-9105.

¿QUE DEBO HACER SI CREO QUE ME HAN ESTAFADO?

Una de las estafas más comunes en Canadá es una estafa de phishing o smishing, donde un estafador se hace pasar por una empresa u organización gubernamental. Por ejemplo, estafas que dicen ser de la Canada Revenue Agency o CRA (Agencia de Ingresos de Canada). A veces, le dice a la victima que debe un saldo elevado, y si no paga, la RCMP vendrá a arrestarla. Otras veces, le dice a la víctima que puede "hacer clic en un enlace para aceptar su reembolso". A algunos simplemente le dice que siga un enlace para revisar los cambios en su información o que llenen un formulario con su información personal.

¿QUE DEBO HACER SI CREO QUE ME HAN ESTAFADO?

Si no está seguro que el mensaje es legítimo, ¡no responda! Visite el sitio web de la organización y llámelos directamente para verificar la información que recibió. Muchos hemos recibido un mensaje fraudulento de CRA que exige el pago de impuestos, la CRA brinda los siguientes consejos:

- La CRA nunca solicita información personal por correo electrónico o mensaje de texto,
- La CRA tampoco solicita pagos con bitcoin o tarjetas de regalo.

Si Usted recibe una llamada, un mensaje de texto o un correo electrónico diciendo que le debe dinero a la CRA, o que se le debe un reembolso o un pago de beneficios, inicie sesión o regístrese en Mi cuenta o Mi cuenta comercial para verificar su estado fiscal, o llame al Ingreso individual de la CRA Línea de consultas fiscales al 1-800-959-8281.

Si es víctima de una estafa, puede haber varios pasos a seguir:

1. Denuncie el fraude a la policía local en su comunidad: Burnaby RCMP's Non-Emergency (24-hour) Tel: 604-646-9999 y sitio web: http://burnaby.rcmp-grc.gc.ca
2. Si le han robado su número de seguro social, comuníquese con Service Canada al 1-800-206-7218 para informarlo.
3. Informe la estafa al **Canadian Anti-Fraud Centre** del RCMP. Se le pedirá que use un FIRMA de inicio de sesión (es decir, su banco) o un GCKey (tal como lo hace para acceder a su cuenta CRA). Esto garantiza su propia seguridad al informar estafas. También puede llamar al Centro Antifraude al 1-888-495-8501.

Los estafadores usan tácticas similares cuando fingen representar a un banco o compañía de tarjetas de crédito. Por ejemplo, puede recibir un correo electrónico o un mensaje de texto de un banco con el que usted no tiene relación pidiéndole que revise su estado de cuenta. Es fácil reconocer el phishing o smishing cuando el mensaje no proviene de su propio banco. Pero, si le preocupa que pueda ser de su banco, no responda al mensaje: comuníquese directamente con el banco por teléfono o en persona o accesando banca en línea (utilizando un sistema seguro conexión a internet, por supuesto) para verificar si es real. Y no olvide informar el mensaje de phishing / smishing a su banco.

Para obtener más información sobre otros incidentes cibernéticos e informes, visite el **Canadian Centre for Cyber Security** (Centro Canadiense de Seguridad Cibernética).

SIGA y OBTENGA SEGURIDAD CIBERNÉTICA EN TWITTER, FACEBOOK E INSTAGRAM

5 Maneras de Protejer su Privacidad en un Dispositivo Inteligente (Telefonos Inteligentes / Tabletas y Relojes Inteligentes)

Estos consejos son para cualquier dispositivo que se conecte a Internet que pueda tener en casa. Los dispositivos conectados (también conocidos como "dispositivos inteligentes") son divertidos y nos hacen la vida más fácil, también brindan oportunidades para que los hackers accedan a información personal y privada. Tome medidas para protegerse usted y a su familia, siguiendo estos consejos:

1. ASEGURE LA RED WI-FI DE SU HOGAR:

Los dispositivos inteligentes utilizan Internet para enviar y recopilar datos. Si la conexión Wi-Fi de su hogar no es segura, ¡sus datos no están seguros! Cuando use Wi-Fi, la seguridad mínima que debe tener es el cifrado inalámbrico y la protección con contraseña. Bajo su configuración inalámbrica, asegúrese de que su enrutador tenga habilitado el cifrado WPA2. Luego, bloquee su red inalámbrica con una contraseña segura y única. Una contraseña segura incluye letras mayúsculas y minúsculas, números y caracteres especiales. Si es un usuario avanzado, cree una zona de red separada en su red Wi-Fi para conectar sus dispositivos inteligentes. Esto se llama "aislamiento del dispositivo" y funciona de manera similar a las redes "Guest Wi-Fi". Cuando use su dispositivo inteligente mientras viaja, conéctese solo a redes confiables y protegidas con contraseña, y desactive las configuraciones que buscan automáticamente redes Wi-Fi.

2. APAGUE LA GEOLOCALIZACIÓN CUANDO NO LA USE:

Muchos dispositivos inteligentes tienen aplicaciones que utilizan la geolocalización para proporcionar servicios, como el seguimiento de la condición física o los mapas. Si una aplicación puede ver su ubicación, un hacker también podría verlo. En la configuración de su dispositivo, desactive la geolocalización cuando no la esté usando.

3. ANTES DE INSTALAR APLICACIONES, ENTIENDA LA POLÍTICA DE PRIVACIDAD Y LOS TÉRMINOS DE USO DE LA APLICACIÓN:

Todas las aplicaciones tienen configuraciones de privacidad que ayudan a controlar quién puede ver su información y lo que ven. Personalice esta configuración de privacidad para que se oculte la información personal, como los nombres completos y datos de contacto. Además, tenga cuidado con las aplicaciones que solicitan información innecesaria o excesiva. Eche un vistazo a los permisos y no haga clic en "permitir" para todo.

4. DESACTIVAR LOS MICRÓFONOS Y CÁMARAS CUANDO NO SE USE:

La mayoría de los auriculares para juegos, televisores inteligentes, relojes inteligentes y altavoces inteligentes vienen con un micrófono y / o cámara. Si no es seguro, su dispositivo podría transmitir información a la que no tiene intención. Apague su cámara y silencie su micrófono cuando no lo esté usando.

5. CREE NOMBRES DE USUARIO QUE NO CONTENGAN INFORMACIÓN

IDENTIFICADORA:
Compartir demasiado puede poner en riesgo su privacidad. Al configurar un inicio de sesión para su dispositivo (o para un juego o aplicación), asegúrese de que su nombre de usuario no contenga información de identificación, como su nombre, edad, ubicación o información de contacto.

6. SEA INTELIGENTE CON EL SMARTPHONE:

Los teléfonos inteligentes pueden rastrear su ubicación y revelar información sobre usted, incluidos sus contactos. Tenga cuidado de descargar y usar solo aplicaciones de buena reputación y asegúrese de proteger con contraseña (o huella digital) su teléfono. Sepa cómo usar las herramientas para buscar o borrar datos personales de teléfonos pérdidos. Encontrará más información en ConnectSafely.org/cellphone-safety-tips.

7. ASEGURE SU ENRUTADOR DE INTERNET:

Es probable que haya un dispositivo pequeño en su hogar, llamado enrutador o módem de banda ancha que lo conecte a Internet. Ese dispositivo tiene una contraseña y un nombre de usuario y, a veces, las contraseñas predeterminadas son muy fáciles de adivinar. Los enrutadores pueden ser difíciles de configurar, por lo que, si tiene dudas, comuníquese con un experto o con su proveedor de servicios de Internet para obtener consejos sobre cómo cambiar la contraseña.

PROTEGE TUS DISPOSITIVOS:

Asegúrese que estén protegidos con contraseña y, en el caso de las computadoras, asegúrese de tener un buen programa de seguridad y firewall. Si necesita ayuda, comuníquese con amigos o familiares bien informados, o con su proveedor de servicios de Internet u operador de telefonía móvil. SHAW y algunos otros proveedores de servicios de Internet pueden ofrecer un software antivirus gratuito, o lo puede comprar u obtener gratuito de una compañía de buena reputación como las que se enumeran en ConnectSafely.org/securityvendors.

OTROS RECURSOS RECOMENDADOS PARA CONSEJOS ADICIONALES VISITA:

FightSpam.gc.ca: Ayuda para que los canadienses y las empresas eviten el spam y otras amenazas electrónicas

Privacidad de los jóvenes: Información y herramientas de la Office of the Privcy Commisioner (Oficina del Comisionado de Privacidad) para ayudar a los jóvenes a proteger su privacidad en línea.

Compras en Línea – Como Protejerse cuando hace Compras por Internet:

UTILICE CONTRASEÑAS FUERTES Y ÚNICAS: Una vez más, las contraseñas seguras son esenciales, al igual que con las cuentas de correo electrónico y redes sociales. Nunca comparta sus contraseñas con nadie, a menos que haya designado a alguien de su confianza para administrar sus cuentas. Asegúrese de que sus contraseñas tengan al menos ocho caracteres. Incluya números, letras mayúsculas y minúsculas y símbolos, y no use nombres ni palabras de diccionario. En ConnectSafely.org/passwords, encontrará consejos e información sobre cómo usar la autenticación multifactor y el reconocimiento de huellas digitales para una seguridad más avanzada.

NO HAGA CLIC EN LOS ENLACES: En el correo electrónico o en las redes sociales de bancos, compañías de tarjetas de crédito, agencias gubernamentales u otras organizaciones, a menos que esté 100% seguro de que son legítimos. Existe una estafa común, llamada phishing, en la que alguien le envía un enlace a lo que parece un sitio web legítimo, pero en realidad es un sitio de estafa creado por delincuentes para robar su información de acceso u otra información personal. Incluso si el nombre de la compañía es parte de la dirección web, aún podría ser una estafa. Su apuesta más segura es escribir la dirección web como lo hace normalmente y, en caso de duda, llamar a la organización.

TENGA CUIDADO CON CUALQUIER OFERTA QUE SEA DEMASIADO BUENA PARA SER VERDAD: Como que le digan que ganó un concurso al que no participó o que le ofrecen un precio increíble en vacaciones o producto muy por debajo de lo que esperaría pagar. Tenga especial cuidado con las ofertas de medicamentos de bajo costo o cobertura médica.

COMPRAR SOLO DE COMERCIANTES REPUTABLES EN LÍNEA: Tenga cuidado con cualquier comerciante en línea del que nunca haya escuchado hablar. Muchos son legítimos, pero algunos podrían robar el número de su tarjeta de crédito u otra información financiera, o simplemente no entregar lo que ha pagado. En caso de duda, pregunte a alguien familiarizado con las compras en línea o investigue en línea para ver si hay informacion o comentarios sobre el comerciante.

CUANDO COMPRE O HAGA TRANSACCIONES BANCARIAS BUSQUE PAGINAS DE INTERNET SEGURAS: Con un *https* en la barra de direcciones del navegador. La "s" significa "seguro". Si es solo http, no es un sitio seguro. Si compra o realiza operaciones bancarias con una aplicación móvil, asegúrese de que haya sido emitida por esa compañía. Busque opiniones de otros o pregunte a un experto si no está seguro.

UTILICE TARJETAS DE CRÉDITO SI ES POSIBLE: De lo contrario, utilice tarjetas de débito o servicios seguros de pago en línea, como Paypal. Nunca envíe efectivo, cheques de caja o giros postales. Incluso enviar cheque personal puede ser peligroso. Es mejor usar una tarjeta de crédito porque, si hay una disputa, la compañía de la tarjeta de crédito detendrá el cargo o le reembolsará su dinero mientras investiga su reclamo. Las tarjetas de débito también tienen protecciones, pero en algunas hay que esperar para recuperar su dinero. Servicios como Paypal, Android Pay y Apple Pay también tienen algunas protecciones, pero las tarjetas de crédito siguen siendo la mejor opción.

TENGA CUIDADO ANTES DE HACER CLIC: Hay ciertas cosas que no podrá deshacer, como

comprar o vender acciones incorrectas o comprar un vuelo no reembolsable o una habitación de hotel. Revise cuidadosamente todas las transacciones antes de confirmarlas. Si comete un error, comuníquese con la compañía de inmediato para ver si es posible deshacerlo. Muchos comerciantes en línea tienen una función de cancelación que le permite cancelar una compra, pero debe hacerlo de inmediato. Una vez que el artículo está listo para ser enviado, puede ser demasiado tarde para cancelar el pedido. A menudo puede devolver sus compras, pero es probable que tenga que pagar por la devolución.

Asegúrese de comprender las políticas de devolución de los comerciantes en línea y conocer todos los cargos, incluídos los gastos de envío, manejo e impuestos.

INVESTIGUE ANTES DE DONAR A CAUSAS EN LÍNEA: Los sitios de financiación colectiva como Kickstarter, Indiegogo y GoFundMe son excelentes lugares para estar entre los primeros partidarios o compradores de nuevos productos, donar a causas y organizaciones dignas, e incluso proporcionar apoyo financiero para personas con una necesidad imperiosa, pero debe proceder con precaución. Lea toda la letra pequeña e investigue un poco sobre la persona u organización detrás de la cause. Si están recaudando dinero para una causa, trate de averiguar si es real, y si están lanzando un nuevo producto genial, asegúrese de que su presentación sea realista. En caso de duda, siga adelante.

PROTEJASE CONTRA EL ROBO DE IDENTIDAD: Nunca ingrese su Número de Seguro Social (SIN) en línea a menos que sepa que se encuentra en un sitio legítimo que tiene una necesidad real de esa información, como solicitar una cuenta bancaria, tarjeta de crédito o préstamo (de un institución) u obtener un informe de crédito. A menos que esté seguro de que es un sitio legítimo, evite publicar su fecha de nacimiento y lugar de nacimiento completos, y tenga cuidado cuando se le pida que ingrese cualquier otra información personal, como su dirección particular. Los sitios de medios legítimos como Facebook e instituciones financieras pueden solicitar su fecha de nacimiento. Solo divulgue números de tarjetas de crédito a comerciantes legítimos en línea. En caso de duda, investigue un poco para ver qué dicen otras personas y comentarios sobre ellos.

MONITOREE SUS CUENTAS FINANCIERAS EN LÍNEA: Busque actividad reciente para asegurarse de que no haya cargos fraudulentos en sus cuentas de crédito, débito o bancarias. Verifique sus cuentas de inversión en línea para asegurarse de que no haya habido actividad no autorizada. Si encuentra algo sospechoso, repórtelo de inmediato al departamento de fraude de la institución financiera o al número gratuito en su tarjeta de crédito o débito. Incluso si no realiza operaciones bancarias en línea, aún existe el riesgo de que pueda ser víctima de fraude. Informe a la institución de inmediato si hay un problema. En la mayoría de los casos, está protegido contra el fraude, pero debe denunciarlo.

ESTAFAS BENEFICAS: La mayoría de las organizaciones benéficas tienen sitios web y la opción de donar en línea. Eso está bien siempre y cuando esté seguro de que está en el sitio correcto y que es una organización benéfica legítima que apoya. Tenga cuidado si recibe un correo electrónico de lo que parece ser una organización benéfica que le pide que haga una donación en línea. Si no está familiarizado con la organización, revise en CharityNavigator.org y si va a donar en línea, asegúrese de ir al sitio legítimo de la organización benéfica. Para estar seguro, ingrese la dirección web de la organización benéfica en el navegador en lugar de hacer clic en un enlace.

Consejos Rápidos para Compras por Internet

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

ALGUNAS PISTAS DE QUE UN SITIO DE COMPRAS NO ES DE CONFIANZA

- El sitio parece mal diseñado, poco profesional y contiene enlaces web rotos.
- No puede encontrar una dirección o el número de teléfono de la empresa.
- Las políticas de venta, devolución y privacidad son difíciles de encontrar o poco claras.
- El botón de retroceso está desactivado. En otras palabras, te quedas atascado en una página y no puedes volver atrás.
- Se le solicita información de la tarjeta de crédito en cualquier momento que no sea cuando realiza una compra.

CÓMO PROTEGERSE CUANDO COMPRAS EN LÍNEA

- Pague con tarjeta de crédito si puede. No envíe dinero en efectivo.
- Esté atento a los precios que son demasiado buenos para ser verdad. Es probable que sean falsificaciones.
- No use el Wi-Fi público para comprar en línea.
- Lea la política de privacidad y descubra cómo se usará su información.
- No responda a un correo electrónico o mensaje emergente que solicite información financiera. Las compañías legítimas no solicitan esta información de esta manera.
- Lea los extractos de su tarjeta de crédito y verifique los cargos no autorizados.
- Asegúrese de que su firewall esté "activado". Por ejemplo, Windows Firewall está activado de forma predeterminada en la última versión de Windows, pero asegúrese de que no esté desactivado:
    - o Abra el Firewall de Windows haciendo clic en el botón Inicio y luego en el Panel de control
    - o En el cuadro de búsqueda, escriba "firewall" y luego haga clic en Firewall de Windows
    - o En el panel izquierdo, haga clic en Activar o desactivar Firewall de Windows
- No permita el autollenado de sus contraseñas o información personal, o escriba su dirección y nunca permita que un sitio almacene la información de su tarjeta de crédito.

Seguridad Para Adultos Mayores: 10 Consejos para evitar ser Víctima de Fraude

(Fuente: https://www.freedomshowers.com/blog/senior-safety-10-tips-avoid-victim-fraud/)

Un día estás disfrutando de una taza de té en casa y suena el teléfono. "Hola abuela, llama tu nieto. He estado viajando y perdí mi billetera y mi pasaporte. ¿Podrías enviarme algo de dinero? ". La voz está un poco apagada, y no puedes decir qué nieto está llamando, pero podrías ofenderlo si lo preguntas. Cada abuela si se le solícita querría ayudar a su nieto a salir de problemas al instante, por lo que también le preguntará dónde enviar el dinero. Desafortunadamente, la persona que llama no es su nieto, sino un estafador dirigido a personas mayores para robar su dinero. Se aprovechan de su naturaleza solidaria.

Llamadas como esta ocurren todo el tiempo robando a las personas su dinero ganado con tanto esfuerzo. La frecuencia de las transacciones fraudulentas aumenta a un ritmo alarmante. El número real es probablemente mucho mayor ya que muchas víctimas de fraude no lo denuncian.

Consejos de prevención

- La policía, los jueces o las entidades legales y gubernamentales nunca solicitarán que se envíe dinero a través de empresas de servicios monetarios.
- Nunca dé información personal a la persona que llama.
- Confirme con otros familiares el paradero del familiar o amigo en cuestión antes de siquiera considerar enviar dinero.
- Nunca envíe dinero a través de servicios de transferencia de dinero a personas que no conoce personalmente. Verifique la identidad de la persona antes de tomar cualquier medida para ayudar. El dinero se puede recoger en cualquier parte del mundo una vez que se le da un número de transacción.

10 CONSEJOS PARA EVITAR SER UNA VÍCTIMA DE FRAUDE:

1. Mi madre me dijo siempre que si **parece demasiado bueno para ser verdad**, probablemente no lo es. Los estafadores prosperan en nuestro deseo de soluciones rápidas, curas milagrosas y dinero fácil. Al ofrecer productos o servicios gratuitos, difíciles de resistir a precios de ganga o grandes premios, atraen a las personas a inscribirse en algo que no desean y los convencen de pagar una tarifa por los gastos de envío o transacción. Estas son estafas con mayor frecuencia, donde toman su "tarifa" y no proporcionan el producto, servicio o premio prometido. **SUGERENCIA: solicite recibir todas las ofertas o detalles de premios por escrito, para que pueda leerlo antes de comprometerse, firmar o aceptar algo. Obtenga una segunda opinión de alguien de su confianza.**

2. Está bien decir "No, gracias" "No en este momento" o "Déjame pensarlo". Las compañías y organizaciones legítimas entenderán si solicitas información por escrito o quieres tiempo para investigar. **CONSEJO: Si se siente presionado para firmar algo o hacer un pago, cuelgue o aléjese.**

3. No divulgue información bancaria, ni tarjetas de crédito, números de seguro social, seguros o números de Medicare por teléfono o internet a personas que llaman o correos electrónicos no solicitados. Una vez más, las compañías legítimas entenderán su diligencia. **SUGERENCIA: solo comparta información personal y financiera con empresas conocidas que haya contactado e investigado**.

4. Tenga cuidado con los encantadores o las personas que suenan oficiales. Los estafadores son inteligentes y saben que muchas personas pueden ser convencidas de entregar dinero o información si

parecen oficiales o son realmente agradables. Los bancos, los oficiales de policía o los funcionarios del gobierno nunca le exigirán que los pague por teléfono o en la puerta. Si alguien le dice que debe dinero, dígale que revisará sus registros y se comunicará directamente con las oficinas. **CONSEJO: vaya a los edificios oficiales para realizar cualquier pago o comuníquese con la organización para confirmar el dinero adeudado.**

5. Los representantes o personas de mantenimiento siempre le notificarán con anticipación si están enviando a alguien a su hogar. **Si algún extraño llama a su puerta, acatue con precaucion.** Si no espera a nadie, no tiene que abrir la puerta. Pídales que regresen más tarde y asegúrese de que no esté solo cuando lo hagan. Si está esperando a alguien, aún debe pedirle que muestre su identificación. Está bien pedirles que esperen afuera, mientras llamas a la compañía de donde provienen para confirmar si han enviado a alguien. Esto incluso se aplica a la policía. **CONSEJO: No permita que personas desconocidas o inesperadas ingresen a su hogar.**

6. Tómese el tiempo para leer la letra pequeña. Muchas personas no leen los términos y condiciones y esto podría ocasionarle problemas o comprometerlo con algo que no desea. Hubo un experimento realizado en Londres hace un par de años, donde las personas aceptaron los términos y condiciones para obtener Wi-Fi gratis, sin leerlo, sin darse cuenta de lo que realmente habían firmado. Lee ese artículo aquí. **SUGERENCIA: nunca firme ningún papel si no comprende completamente lo que está firmando.**

7. Verifique la legitimidad de cualquier empresa, organización, concurso o persona que le solicite información o dinero, antes de registrarse o pagar cualquier cosa. Asegúrese de que estén registrados y o con licencia local. Consulte con el Better Business Bureau si ha habido quejas anteriores. La mayoría de las compañías legítimas tendrán un sitio web, una dirección y con suerte, algunas comentarios de clients, pero tenga en cuenta que incluso esa información puede ser falsa. En caso de duda, pregunte por ahí. Si está en las redes sociales como Facebook, pregunte a sus amigos y familiares si conocen la empresa. **CONSEJO: Asegúrese de saber a quién le está dando su dinero o información también, y si son confiables.**

8. Sea un consumidor informado. Tómese el tiempo para darse una vuelta, comparar precios y calidad. Haga muchas preguntas y verifique la información que un vendedor le está diciendo. **CONSEJO: Investigue antes de comprar. Asegúrese de obtener lo que quiere y necesita.**

9. Nunca transfiera dinero a alguien que no conoce. Las transferencias bancarias son casi imposibles de rastrear, rastrear o revertir. Es como enviar dinero en efectivo, lo que lo convierte en una de las mejores formas para que un estafador se salga con la suya. De todo el dinero perdido por los estafadores en 2014, el 30% se envió a través de transferencias bancarias. Otro 30% de los consumidores pagaron a los estafadores con tarjetas de regalo prepagas. **SUGERENCIA: si alguien le pidió que le pague a través de un método que no se puede rastrear y no es reembolsable, sospeche y no pague.**

10. Si descubre que ha sido víctima de fraude, denúncielo a la policía. Con demasiada frecuencia, el fraude no se denuncia porque las personas se avergüenzan de que "cayeron en la trampa" o "deberían haberlo sabido mejor". La verdad es que los estafadores son buenos en lo que hacen, y si fue víctima de sus técnicas extremadamente convincentes, no hizo nada malo. Si lo denuncia, es posible que tenga

una pequeña posibilidad de recuperar fondos perdidos y tal vez pueda salvar a otra persona de delitos similares. Además, si cree que alguien ha obtenido acceso a información confidencial, notifique a sus instituciones financieras para ver qué se puede hacer para protegerlo.

Que Debo Hacer Si pienso que me han Estafado o He sido Víctima de Fraude?

Todos los frauds y estafas deben ser reportados, incluso si está avergonzado o siente que la cantidad de dinero es demasiado pequeña para preocuparse. Si bien es posible que no pueda recuperar su dinero, puede evitar que el estafador engañe a otras personas. Puede informar todos los fraudes y estafas a:

1. La policía local en su comunidad: Burnaby RCMP's **Non-Emergency (24-hour)** Tel: 604-646-9999 y sitio web: http://burnaby.rcmp-grc.gc.ca

2. Canadian Anti-Fraud Centre (CentroCanadiense contra el Fraude en Canadá): **Número gratuito 1-888-495-8501 o visite el sitio web:** https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/report-fraud .html

3. **Financial Consumer Agency of Canada (FCAC)** (Agencia del Consumidor Financiero de Canadá): proporciona información sobre sus derechos al tratar con bancos y otras instituciones financieras. Tel: 1-866-461-3222 (TTY 613-947-7771, o 1-866-914-6097), sitio web: fcac.gc.ca

4. Para obtener más información, visite Canada.ca/Seniors o visite su oficina local de Service Canada.

PASOS PARA REPORTAR UN FRAUDE, O UNA ESTAFA:

Paso 1: Reúna toda la información que tenga sobre el fraude. Esto incluye documentos, recibos y copias de correos electrónicos o mensajes de texto.

Paso 2: Informe el incidente a la policía local. Esto garantiza que sepan qué estafas están dirigidas a sus residentes y empresas. Mantenga un registro de todas sus llamadas y registre todos los archivos o números de ocurrencia.

Paso 3: Comuníquese con el Centro Canadiense contra el Fraude, por teléfono Tel: 1-888-495-8501 Horario de atención: lunes a viernes de 9:00 a.m. a 4:45 p.m. (hora del este)

Paso 4: Informe el incidente a la institución financiera donde se envió el dinero (por ejemplo, negocios de servicios monetarios como Western Union o MoneyGram, banco o cooperativa de crédito, compañía de tarjetas de crédito o proveedor de servicios de pago por Internet).

Paso 5: Si el fraude ocurrió en línea a través de Facebook, eBay, un anuncio clasificado como Kijiji o un sitio web de citas, asegúrese de informar el incidente directamente al sitio web. Estos detalles se pueden encontrar en "informar abuso" o "informar un anuncio".

Paso 6: Las víctimas de fraude de identidad deben colocar banderas en todas sus cuentas e informar a las agencias de crédito, Equifax https://www.consumer.equifax.ca/personal/ y TransUnion https://www.transunion.ca /

18 Consejos de Seguridad en Internet para Adultos Mayores

(Fuente: http://www.vistaspringsliving.com/blog/18-internet-safety-tips-for-seniors)

SEGURIDAD Y SEGURIDAD GENERALES:

1. Asegúrese de que sus contraseñas sean únicas y seguras. Utilice contraseñas seguras que no incluyan información personal e intente evitar palabras del diccionario y frases comunes. Muchos sitios web recomiendan una combinación de letras mayúsculas y minúsculas, números y símbolos. Además, nunca use la misma contraseña para más de una cuenta.

2. Utilice programa antimalware y otras herramientas de protección. Asegúrese de que su computadora tenga algún tipo de software de seguridad confiable instalado y configúrelo para que se actualice automáticamente para que esté protegido contra los últimos riesgos. Pregúntele a un experto o persona de confianza en tecnología si no está seguro de qué instalar.

3. No descargue archivos adjuntos desconocidos y programas. Nunca descargue documentos, imágenes o software si no conoce y no confía en la fuente. Los estafadores y los hackers a menudo disfrazan los virus y otro malware como herramientas de programa "gratuitos" o contenido interesante para descargar.

4. Considere autorizar a un amigo o familiar de confianza para acceder a sus cuentas. En caso de emergencia, puede ser difícil o imposible para amigos y familiares de confianza acceder a cuentas de correo electrónico, bancos y almacenamiento de archivos en línea. Planifique con anticipación y trabaje con un abogado para autorizar a alguien de su confianza a acceder a sus cuentas.

CORREO ELECTRÓNICO Y MEDIOS SOCIALES:

5. Entender los filtros de "spam". **El spam se refiere a correos electrónicos no deseados y no solicitados. La mayoría de los proveedores de correo electrónico tienen filtros de spam que eliminan estos correos electrónicos de su bandeja de entrada principal.**

6. Use la configuración de privacidad de las redes sociales. Tenga en cuenta lo que está publicando en cualquier sitio de redes sociales y use la configuración de privacidad para restringir el acceso a sus publicaciones a las personas de su confianza con información personal.

7. Reporte cualquier y todos los casos de abuso. El acoso cibernético puede estar asociado con niños y adolescentes, pero eso no significa que los adultos no sean maltratados en línea. No responda. En cambio, denuncie el abuso, tanto a la plataforma en la que se encuentra como a las personas que pueden ayudar, y recuerde que el abuso no es su culpa.

8. Conozca los signos de una estafa. Si es demasiado bueno para ser verdad, generalmente no lo es. Las ofertas de artículos de alto precio gratuitos o de bajo precio, como vacaciones, productos electrónicos y medicamentos, generalmente son intentos de estafa. Por otro lado, los estafadores a veces le envían solicitudes de dinero de las cuentas personales de sus amigos; nunca responda ni envíe fondos sin antes verificar la solicitud con la persona de alguna otra manera.

DINERO Y COMPRAS:

9. Busque sitios de internet seguros. Siempre que se le solicite ingresar su información de pago en un sitio web, primero verifique que el sitio web sea seguro. En la barra de URL en la parte superior de su navegador de

Internet, busque "https: //" para un sitio seguro. (La "s" significa seguro).

10. Comprenda y evite los intentos de phishing. Tenga cuidado con los enlaces a sitios que le piden que realice una compra o ingrese su información de pago. Una estafa común, "phishing", hace que un sitio falso se vea como un sitio confiable, luego le da su información al estafador. Busque errores gramaticales, errores ortográficos y URL que se vean diferentes de lo que está acostumbrado. En caso de duda, ingrese la dirección de internet que sabe que es correcta directamente en la barra de URL.

11. No ingrese información personal o de pago en un sitio desconocido. Igualmente, asegúrese de verificar el sitio de internet si va a ingresar información personal o de pago. Busque reseñas de minoristas en línea y, en el caso de los portales bancarios o gubernamentales, nunca responda a las solicitudes de información. Los bancos y las agencias gubernamentales ellos nunca solicitarán contraseñas, números de Seguro Social o información de pago.

12. Controle sus cuentas financieras. Incluso cuando toma todas las precauciones, existe la posibilidad de que su información de pago se filtre o sea robada de un proveedor confiable. Mire sus cuentas bancarias y tarjetas de crédito para compras no autorizadas.

CONOCIENDO NUEVAS PERSONAS:

13. Tenga precaución. Desafortunadamente, no todos en Internet son quienes dicen ser. Hay muchas oportunidades en línea para conocer gente nueva, desde sitios de citas hasta grupos de pasatiempos y foros, pero no todos son confiables. Sea cauteloso cuando interactúe con nuevas personas y no brinde demasiada información personal donde las personas puedan encontrarla.

14. No envíe dinero a nuevos conocidos. De manera similar a la información personal, algunas personas utilizarán el relativo anonimato de Internet para acercarse a sus objetivos, luego solicitarán dinero y nunca más volverá a saber de ellos. No se deje llevar por historias de tragedias personales o solicitudes de dinero para visitarla(o) a menos que sea positivo de las buenas intenciones de la persona.

15. Cuando se reúnan en persona, esté protegido. Si elige conocer a alguien de un sitio de internet de citas o un amigo que conoció en línea, elija un lugar público y dígale a un amigo o familiar a dónde va y con quién se va a reunir. Nunca puede estar demasiado seguro, incluso si siente que conoce bien a la persona.

BIENESTAR Y SALUD:

16. Conocer los hechos de la ficción. Los sitios de internet como los editores de noticias y los blogs de consejos de salud a menudo ganan dinero al atraer a los visitantes a ver y hacer clic en anuncios en sus páginas, y publicarán titulares sensacionales para obtener esas vistas. No todo lo publicado en un sitio internet es cierto, no importa cuán oficial pueda parecer.

17. Evite el autodiagnóstico y los consejos de salud en el sillón. Es increíblemente fácil buscar sus síntomas en un búscador y encontrar una lista de posibles enfermedades, o un foro que discuta un diagnóstico. Solo un profesional de la salud con licencia que comprenda sus antecedentes de salud debe hacer diagnósticos y prescribir tratamientos. Intentar usar Internet para hacerlo podría significar que la afección no se trata o empeora.

18. Seguimiento con un profesional. Por supuesto, no todos los consejos de salud en Internet son de vida o muerte. Hay muchos recursos útiles en línea para consejos nutricionales, bienestar y buena forma física, pero siempre es bueno consultar a un profesional (médico, enfermero, dietista y nutricionista) antes de hacer cualquier cambio que pueda afectar su salud, como un nuevo plan de dieta o ejercicio.

Al educarte a ti mismo, puedes mantenerte seguro. Aquí hay algunos otros recursos que puede consultar:
Guía de seguridad para personas mayores de RCMP: http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7
Cómo protegerse mientras compra en línea: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx

Guias y consejos básicos en línea: https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice Compras, banca, caridad y viajes en línea - https://www.connectsafely.org/seniors /
Los 10 mejores consejos para proteger su bandeja de entrada, computadora y dispositivo móvil: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/