Competition Bureau Canada | Bureau de la concurrence Canada

EL PEQUEÑO LIBRO NEGRO DE LAS ESTAFAS

Canada

EL PEQUEÑO LIBRO NEGRO DE LAS ESTAFAS

SEGUNDA EDICIÓN

Publicado por primera vez por la Competition Bureau Canada (Oficina de la Competencia de Canadá), 2012

La presente publicación no es un documento jurídico. Su objetivo es ofrecer información general y se proporciona para su conveniencia.

Para más información sobre las actividades del Competition Bureau, contacte a:

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

Tel.: 819-997-4282
Número gratuito: 1-800-348-5358
Teléfono de texto (para personas sordas): 1-866-694-8389
Fax: 819-997-0324
Sitio web: www.competitionbureau.gc.ca

Para obtener una copia de esta publicación, o recibirla en un formato alternativo (sistema braille, letras grandes, etc.), contacte con el Centro de Información del Competition Bureau llamando a los números de contacto enumerados más arriba.

Esta publicación también está disponible en línea en HTML en la siguiente dirección:
http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

Permisos de reproducción

Cat. No. Iu54-42/2018Sp-PDF
ISBN: 978-0-660-29918-1
2019-03-29

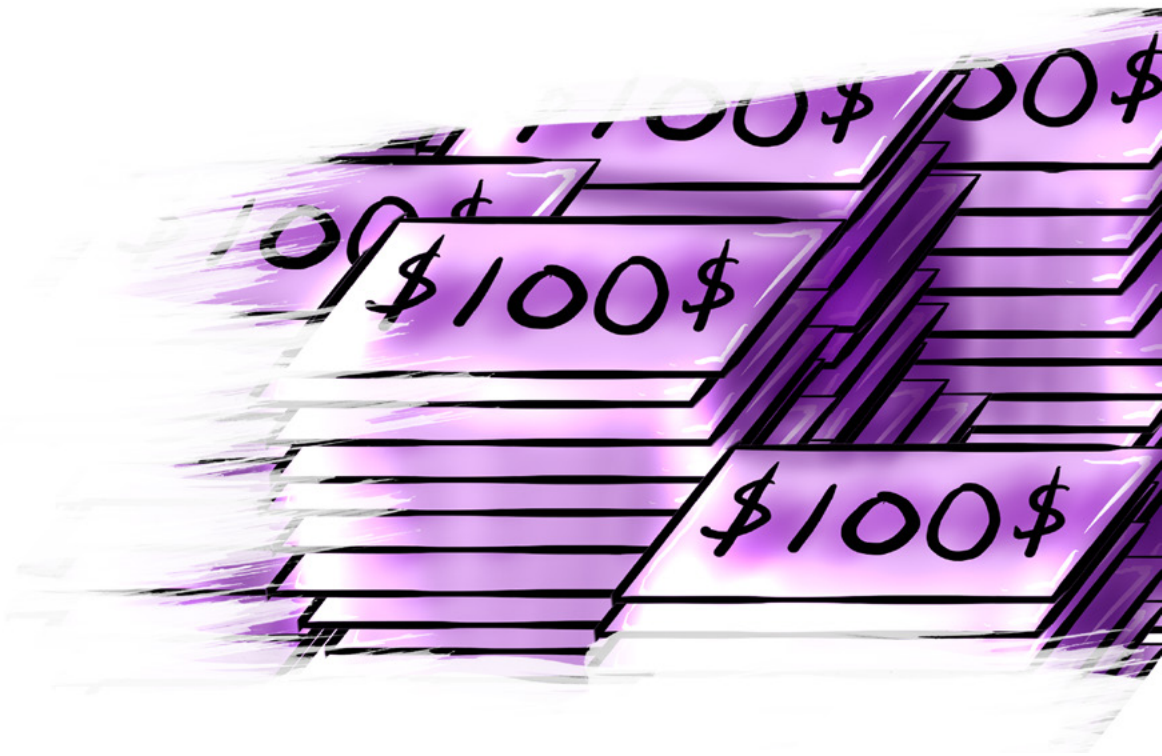
This publication is available through PDF on the web in the following languages: English, Chinese simplified, Chinese traditional, Punjabi, French, Tagalog.

PRÓLOGO

Los estafadores son sigilosos y astutos. Su objetivo puede ser cualquier persona, desde joven a jubilada. Su objetivo también puede ser un negocio. Nadie es inmune a la estafa.

Nuestro grupo de superhéroes ha encontrado una manera de desenmascarar los timos. Su secreto es simple: ¡el conocimiento es poder!

Lea este texto para descubrir cómo usted también puede convertirse en superhéroe que lucha contra las estafas. ¡Comparta este folleto con su familia y amigos y recobre el poder!



ÍNDICE

PUNTOS BÁSICOS PARA LA LUCHA CONTRA EL FRAUDE

Conviértase en un superhéroe de la vida real al armarse con la información necesaria para luchar contra las estafas y mantenga a salvo a su familia, su dinero y a usted mismo.

Usted trabaja duro para conseguir su dinero. Y quiere gastarlo en las cosas que le importan, ya sea la educación de sus hijos, un viaje emocionante o un nuevo *smartphone*.

Los estafadores son reales. Están ahí, cada día buscando nuevas víctimas. Tratarán de estafarle en línea, por teléfono, por correo o en persona.

Usted puede ser su objetivo. Miles de canadienses pierden millones de dólares cada año debido a los estafadores. El impacto de las estafas sobre las familias y los negocios puede ser devastador.

Aprenda a luchar contra las estafas. Este folleto incluye 12 de las estafas más comunes por las que actualmente se ven afectados los canadienses. Se presentan muchos consejos y trucos que enseñan cómo protegerse a uno mismo y qué puede hacer si es víctima de una estafa.

¡Denúncielo! Cualquier persona puede sufrir una estafa, desde los adolescentes a los abuelos, pasando por los altos directivos empresariales. Lo mejor que puede hacer es denunciar la estafa, sea cual sea la cantidad, ante las autoridades competentes. No se sienta avergonzado; al denunciar estará ayudando a que otras personas no caigan en la estafa.

El conocimiento es su poder. Protéjase buscando más información. Además de este folleto, también puede consultar numerosas páginas web de confianza para conseguir más información.

El Canadian Anti-Fraud Centre (Centro Canadiense de Lucha contra el Fraude), gestionado por la Real Policía Montada de Canadá (RCMP, por sus siglas en inglés), el Competition Bureau y la Policía Provincial de Ontario cuentan con mucha información sobre las estafas. ¡Amplíe sus conocimientos hoy mismo visitando www.antifraudcentre.ca!

ESTAFA DE SUSCRIPCIÓN

¡Una buena oferta puede hacer que caiga en una trampa muy cara!

Una estafa de suscripción puede engañarle ofreciéndole periodos de prueba "gratuitos" o "a bajo costo" para diferentes productos y servicios. Entre los productos ofrecidos se suelen encontrar pastillas para adelgazar, alimentos saludables, medicamentos y productos anti-edad.

Una vez que proporciona la información de su tarjeta de crédito para cubrir los gastos de envío, se verá atrapado en una suscripción mensual sin saberlo. Será muy difícil, si no imposible, parar los envíos y los cobros.

Los estafadores utilizan páginas web, correos electrónicos, redes sociales y teléfonos para atrapar a sus víctimas. Recuerde, las tácticas de venta de alta presión, como una "oferta por tiempo limitado", a menudo se utilizan para hacerle tomar una decisión precipitada.

Consejos para protegerse:

- **Confíe en sus instintos. Si es demasiado bueno para ser cierto, no se registre ni inscriba.**
- **Antes de registrarse para una prueba gratuita, investigue la empresa y lea opiniones de otros usuarios, sobre todo los negativos. El Better Bussines Bureau (Agencia de Mejores Negocios, BBB) es una gran fuente de información.**
- **No se inscriba si no puede encontrar o entender los términos y condiciones. Preste especial atención a las casillas premarcadas, a las cláusulas de cancelación, las políticas de devolución y a cualquier cargo poco claro.**
- **Si va adelante con la prueba gratuita, conserve todos los documentos, recibos, correos y mensajes de texto.**
- **Compruebe regularmente los extractos de su tarjeta de crédito para revisar si hay cargos frecuentes o desconocidos.**
- **Si tiene problemas para cancelar su suscripción, contacte a su proveedor de tarjeta de crédito, su organización local de protección de los consumidores o a los organismos policiales.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para encontrar más información.

ROBO DE IDENTIDAD

¡Contribuya a asegurar que su identidad siga siendo solamente suya!

Los estafadores están siempre al acecho, tratando de recopilar o reproducir su información personal para cometer fraude. Los ladrones pueden realizar compras usando sus cuentas, obtener pasaportes, recibir ayudas del gobierno, solicitar préstamos y mucho más. Esto puede trastornar su vida por completo.

Los estafadores usan técnicas que van desde lo más simple a lo más elaborado. En el mundo analógico, pueden hurgar en la basura o robar el correo. En línea, pueden usar programas espía y virus, así como otros delitos informáticos como el pirateo [*hacking]* y fraude electrónico [*phishing*] (ver la página 13).

Buscan información sobre las tarjetas de crédito, detalles de la cuenta bancaria, el nombre completo y la firma, la fecha de nacimiento, el número de seguridad social, la dirección completa, el nombre de soltera de su madre, nombres de usuario y contraseñas, el número de la licencia de conducir y el número de pasaporte.

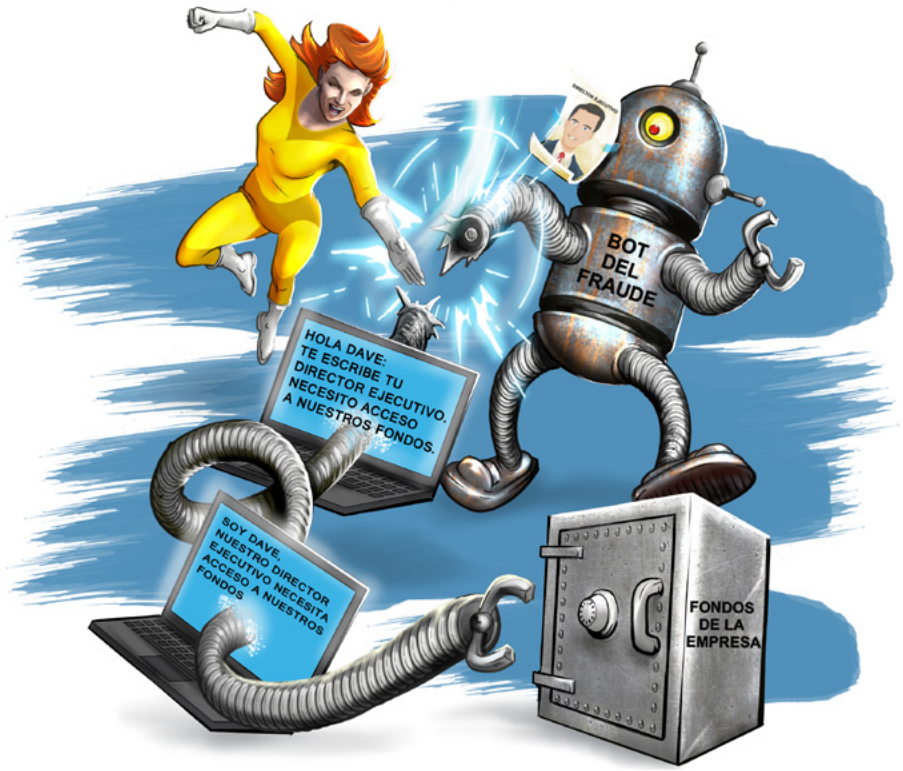
¡El robo de identidad es un delito grave!

Consejos para protegerse:

- **Nunca facilite su información personal por teléfono, por mensaje de texto, correo electrónico o Internet.**
- **Evite el uso de computadoras públicas o redes Wi-Fi públicas, como en las cafeterías, para acceder o introducir su información personal; esto le puede poner en peligro.**
- **Cree contraseñas fuertes y únicas para cada una de sus cuentas en línea. Proteja con contraseñas sus dispositivos y su red de Wi-Fi doméstica.**
- **Utilice un servicio de pago seguro y de confianza cuando compre en línea (busque una URL que comience con "https" y el símbolo de un candado cerrado).**
- **Evite dar su información personal en redes sociales. Podría ser utilizada junto con sus fotografías para cometer estafas.**
- **Siempre resguarde su número PIN cuando utilice su tarjeta. Si se la entrega a un/a cajero/a, nunca pierda la tarjeta de vista.**
- **Triture y destruya los documentos con información personal.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.



ESTAFAS DE DIRECTORES EJECUTIVOS

Su director ejecutivo le pide dinero urgentemente; ¡asegúrese de que el correo electrónico es auténtico!

¿Trabaja en contabilidad o finanzas? ¿Tiene autoridad para manejar dinero en el trabajo? ¿Está bajo las órdenes de un director ejecutivo (CEO, por sus siglas en inglés)? Si es así, esté alerta; ¡este fraude se dirige a usted particularmente!

En una "estafa de director ejecutivo" típica, los estafadores se harán pasar por un directivo de la empresa, bien consiguiendo acceso a su correo electrónico o imitándolo.

Le enviarán correos con apariencia realista con los que tratarán de engañarle para que envíe dinero a una tercera parte.

Los correos harán que la petición parezca urgente y confidencial. Por ejemplo, podrían decirle que necesitan el dinero para asegurar un contrato importante, llevar a cabo una transacción confidencial o actualizar la información de pago de un proveedor.

Cuando se trata de este tipo de correos, los estafadores normalmente siguen una estrategia con el tiempo bien programado. Los envían cuando los directivos están fuera o cuando es difícil contactar con ellos. Esta lucrativa estafa puede costar a las empresas desde decenas de miles a millones de dólares.

Las estafas de directores ejecutivos constituyen una amenaza global creciente que se dirige por igual a los pequeños negocios locales y a las grandes empresas.

Consejos para protegerse:

- **Mantenga sus sistemas informáticos seguros con un antivirus de confianza actualizado y utilice contraseñas fuertes.**
- **Compruebe todas las peticiones de envío de dinero por teléfono o en persona. Nunca use la información de contacto proporcionada en los correos electrónicos.**
- **Verifique la dirección de correo electrónico del remitente: los estafadores a menudo crean direcciones que son muy similares a las auténticas, con tan solo una o dos letras de diferencia.**
- **Anime a su compañía a crear procesos estandarizados para los envíos de dinero que requieran múltiples niveles de aprobación.**
- **Limite los detalles que comparte públicamente. Los estafadores utilizan la información que está disponible en línea y en las redes sociales para encontrar potenciales víctimas y para programar sus estafas.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS MÉDICAS Y DE SALUD

Tenga cuidado con las curas mágicas que ofrecen soluciones rápidas y fáciles.

Hay estafadores que esperan beneficiarse del sufrimiento de las personas. Los tres tipos más comunes de estafas de salud son las curas mágicas, los programas de adelgazamiento y las farmacias en línea falsas. Estas estafas a menudo aparecen como anuncios patrocinados en las redes sociales o como ventanas emergentes en las páginas web.

Los estafadores ofrecen productos y servicios que parecen ser medicinas alternativas y tratamientos auténticos que combaten enfermedades graves de forma rápida y fácil. Algunos de ellos parecen estar respaldados por famosos o promovidos por testimonios de personas que dicen haber sido curadas.

Las estafas de adelgazamiento prometen espectaculares resultados con poco o ningún esfuerzo. Los estafadores pueden promover dietas inusuales; ejercicios revolucionarios; dispositivos quemagrasas o productos innovadores, como píldoras, parches o cremas.

Las farmacias en línea falsas ofrecen fármacos y medicamentos a precios muy bajos o sin necesidad de receta médica. Se anuncian en Internet y envían correos electrónicos basura (*spam*). Aunque reciba los productos prometidos, no hay garantías de que sean reales o que sea seguro tomarlos.

Consejos para protegerse:

- **Recuerde que no hay píldoras mágicas o curas milagrosas para adelgazar rápidamente o para tratar enfermedades.**
- **No confíe en anuncios de suplementos, medicamentos. Obtenga la información correcta de su profesional de atención médica.**
- **Nunca se comprometa a nada bajo presión, sobre todo si se requiere el pago adelantado de una cantidad elevada o un contrato a largo plazo.**
- **Recuerde que, si una farmacia en línea es legítima, necesitará recetas válidas.**
- **Desconfíe de los apoyos o testimonios de los famosos.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS ROMÁNTICAS

¿Quién está realmente al otro lado de la pantalla?

Manténgase alerta y preste atención a potenciales estafadores que tratarán de bajar sus defensas apelando a su lado más romántico y compasivo. Pueden buscar víctimas tanto en los sitios de citas populares y auténticos como en los falsos.

En un sitio de citas real, un estafador podría enviarle unos cuantos mensajes con una vistosa foto de sí mismo, o de alguien quien dice ser. Una vez que usted se sienta atraído por esa persona, empezará a pedirle que le envíe dinero. Los estafadores pueden decir que tienen un familiar muy enfermo o una situación desesperada para la que necesitan su ayuda. Una vez que usted les da el dinero, suelen desaparecer.

Un estafador también puede llegar a crear un sitio de citas falso en el que usted tiene que pagar por cada mensaje que envía y recibe. Para hacer que usted vuelva a escribir y a pagar, el estafador puede servirse de mensajes ambiguos sobre el amor y el deseo que siente por usted.

En muchos casos el estafador puede incluso acordar una cita para conocerle en persona y hacer que la estafa sea aún más creíble.

Consejos para protegerse:

- **Nunca envíe dinero ni facilite información financiera en un sitio de citas.**
- **Confíe en sus instintos, haga preguntas y lea cuidadosamente los términos y condiciones antes de registrarse.**
- **Sepa qué servicios son gratuitos, cuáles cuestan dinero y qué se necesita para cancelar su cuenta.**
- **Asegúrese de utilizar solo sitios de citas auténticos y fiables. Compruebe siempre cuidadosamente las direcciones de los sitios web, ya que los estafadores a menudo imitan direcciones web reales.**
- **Recuerde que es muy improbable que alguien declare su amor eterno a otra persona tras haber intercambiado únicamente unas pocas cartas, correos electrónicos, llamadas de teléfono o fotografías.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS A LAS EMPRESAS

¡Esté al día con los mecanismos de estafa que se dirigen a los negocios!

Las organizaciones de cualquier tamaño pueden ser engañadas por ingeniosas estafas, así que asegúrese de estar informado.

Una habitual es el fraude del directorio. El estafador envía a su compañía una propuesta para que se anuncie en una revista, periódico, o en un directorio empresarial o en línea. Le llamarán para confirmar la dirección y otros detalles. Después, el departamento de contabilidad recibirá y pagará la factura, sin saber que su compañía nunca ordenó o autorizó el servicio realmente.

Otra estafa común es la de los productos de salud y seguridad. Es posible que reciba una llamada de alguien que dice ser del gobierno provincial, indicándole que sus botiquines de primeros auxilios tienen que ser sustituidos, o que tiene que actualizar la capacitación en materia de salud y seguridad de la compañía. En ambos casos, se le suele pedir que actúe rápidamente.

Otra posible estafa es la de los suministros de oficina, que consiste en que usted recibe y se le cobra por artículos que nunca solicitó.

En muchos casos, los estafadores le acosarán para que pague la cantidad que le reclaman. Incluso le engañarán para hacerle creer que enviarán su información a una agencia de cobros.

Consejos para protegerse:

- **Esté informado de estas posibles estafas e informe a sus empleados y a sus colaboradores para que actúen con cautela ante las llamadas no deseadas.**
- **Cree una lista de las compañías que se utilizan normalmente en su negocio.**
- **Limite el número de personas con autorización para aprobar compras y pagar facturas.**
- **Defina claramente los procedimientos de verificación, pago, y gestión de las cuentas y las facturas.**
- **Contacte con el regulador de su provincia para saber cuáles son sus obligaciones legales.**
- **Los estafadores utilizarán nombres y logotipos de compañías similares a aquellos utilizados por las empresas conocidas para hacer que sus facturas parezcan reales. Revise cuidadosamente las facturas antes de realizar cualquier pago.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE *PHISHING* Y *SMISHING*

Esté alerta. ¡Los mensajes se fabrican con facilidad!

A medida que pasamos más tiempo en línea, los estafadores se vuelven más creativos con las estafas en el espacio digital.

El *phishing* consiste en que usted recibe un correo no deseado que dice proceder de una organización legítima, como una institución financiera, una empresa o una agencia del gobierno. Los estafadores le piden que proporcione o verifique información personal o financiera (como su número de tarjeta de crédito, las contraseñas o el número de la seguridad social) por correo electrónico o haciendo clic en un enlace en Internet.

El *smishing* es lo mismo pero a través de los mensajes de texto (SMS). Estos mensajes suelen copiar el tono y el logotipo de las organizaciones en las que usted confía, y generalmente incluyen una llamada a la acción. Adoptan diversas formas y maneras pero todas ellas persiguen acceder a sus detalles personales.

Consejos para protegerse:

- **Recuerde que las organizaciones fiables nunca le pedirán información personal por correo electrónico o mensaje de texto.**
- **Ignore las comunicaciones procedentes de contactos desconocidos.**
- **Elimine los mensajes sospechosos ya que pueden contener virus.**
- **No responda a correos spam, ni siquiera para anular la suscripción, y no abra ningún documento adjunto ni haca clic en ningún enlace.**
- **Para verificar un hipervínculo sin pulsar en él, pase su ratón por encima. Compruebe cuidadosamente si es correcto.**
- **Actualice su software antivirus en todos los dispositivos.**
- **No utilice nunca el número de teléfono o la dirección de correo electrónico proporcionado en el mensaje sospechoso. Use la información de contacto mostrada en los sitios web verificados.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE IMPUESTOS

¿Ha recibido una llamada o correo electrónico de la CRA? ¡Asegúrese de que es real!

Usted recibe un mensaje de texto de la Agencia de Ingresos de Canadá (Canada Revenue Agency, CRA) que asegura que usted tiene derecho a recibir una devolución extra y que todo lo que debe hacer es proporcionar sus datos bancarios. Tenga cuidado, las estafas de impuestos suenan exactamente así: como situaciones demasiado buenas para ser reales.

Otra variante consiste en que le llaman para decirle que usted debe dinero a la CRA y que necesita pagar inmediatamente, y si no lo hace, le denunciarán a la policía.

En cualquier caso, si usted recibe una llamada, carta, correo electrónico o mensaje de texto diciendo que debe dinero a la CRA, puede confirmarlo en línea entrando en "My Account" o llamando al 1-800-959-8281.

Consejos para protegerse:

La CRA nunca:

- **utilizará un lenguaje agresivo o amenazante.**
- **le amenazará con arrestarlo o con llamar a la policía.**
- **solicitará pagos a través de tarjetas de prepago o tarjetas de regalo, como las de iTunes, Home Depot, etc.**
- **aceptará o enviará pagos a través de Interac o e-transfer.**
- **usará mensajes de texto para comunicarse bajo ninguna circunstancia.**

Los correos electrónicos de la CRA:

- **nunca piden información financiera.**
- **nunca proporcionan información financiera.**

Los modos de pago aceptados por la CRA son:

- **la banca en línea.**
- **las tarjetas de débito.**
- **el débito preautorizado.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE PUERTA A PUERTA

–¡Toc, toc! –¿Quién es? –Un estafador

Aunque vivimos en la era digital, todavía hay algunas estafas a la antigua usanza que llegan directas a su puerta y que pueden suponer una amenaza para usted y su negocio. Con este engaño, los vendedores puerta a puerta utilizan tácticas de alta presión para convencerle de que compre un producto o se suscriba a un servicio que no desea o no necesita.

Estos discursos agresivos a menudo se basan en donaciones benéficas, oportunidades de inversión o servicios domésticos y de mantenimiento de diversos dispositivos, como calentadores de agua, calderas o aparatos de aire acondicionado.

En muchos casos, nunca recibirá el producto o el servicio prometido.

En otros, los productos o servicios son de baja calidad o no coinciden con lo mostrado.

Consejos para protegerse:

- **No se sienta presionado para tomar una decisión rápida. Tómese un tiempo para averiguar más sobre el vendedor y los productos.**
- **Solicite una identificación con fotografía, pida el nombre de la persona y de la empresa u organización benéfica a la que representa.**
- **Pida saber cómo se distribuyen o asignan los fondos de la organización benéfica. Asegúrese de tener esta información por escrito.**
- **Nunca comparta información personal o copias de facturas o extractos bancarios.**
- **Solo permita acceder a su propiedad a aquellas personas en las que confíe.**
- **Investigue antes de invertir. No firme nada y lea siempre la letra pequeña.**
- **Conozca sus derechos. Contacte con su oficina local de defensa de los consumidores; la mayoría de las provincias y territorios tienen directrices conforme a ley de protección de los consumidores.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE EMERGENCIA

Los abuelos que cuidan de sus nietos no deben actuar demasiado rápido.

Las estafas de emergencia generalmente se dirigen a los abuelos cariñosos, aprovechándose de sus sentimientos para robarles su dinero.

La típica estafa comienza con un abuelo que recibe una llamada telefónica de alguien que dice ser su nieto. El "nieto" asegura que está en peligro (las desgracias habituales incluyen el haber sufrido un accidente de tráfico, estar en la cárcel, o tener problemas para regresar de un país extranjero) y que necesita dinero inmediatamente.

La persona que llama le hará preguntas, tratando de que usted revele información personal. También le rogará que mantenga el secreto, ya que se siente avergonzada y no quiere que otros familiares sepan lo que ha pasado.

Otra variante consiste en que hay dos personas al teléfono, una fingiendo ser el nieto y la otra un policía o abogado.

En otros casos, el estafador fingirá ser un antiguo vecino o un amigo de la familia con problemas.

Consejos para protegerse:

- **Tómese su tiempo para verificar la historia. Los estafadores confían en que usted querrá ayudar rápidamente a su ser querido en un caso de emergencia.**
- **Llame a los padres del niño o a los amigos para conocer los detalles.**
- **Pregunte a la persona al teléfono cosas que solo podría responder su ser querido y verifique su identidad antes de tomar medidas para ayudarle.**
- **Nunca envíe dinero a personas que no conoce y en las que no confía.**
- **Nunca dé información personal a la persona que llama.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE COMPRA DE PRODUCTOS

¡No todos los vendedores en línea son de confianza!

Realizar compras en línea es uno de los pasatiempos favoritos de muchos consumidores. Pero muchas de las promociones que puede encontrar en línea, desde bolsos de diseño baratos a productos electrónicos con grandes descuentos, son demasiado buenas para ser ciertas.

Los estafadores pueden crear cuentas en sitios de subastas legítimos, como eBay, o en un mercado de venta en línea, como Kijiji o Craigslist. Anunciarán sus productos a precios muy bajos, incitándole a que los compre.

Y, después de todo, si recibe algo, podría ser de mala calidad o una mala imitación de lo que usted esperaba.

En otros casos, los estafadores le engañarán para que pulse en enlaces patrocinados que le dirigirán a un sitio web aparentemente auténtico. Si decide comprar desde ahí, no tendrá ninguna protección ni servicios que los sitios auténticos sí ofrecen.

Si un sitio o una oferta destaca considerablemente sobre el resto, lo más probable es que algo no esté bien.

Consejos para protegerse:

- **Adquiera productos de compañías o individuos a los que conoce por su reputación o experiencias pasadas.**
- **Nunca haga negocios fuera del sitio de subastas.**
- **Desconfíe de los vendedores de lugares lejanos o que tengan pocos o ningún comentario de otros usuarios.**
- **Utilice una tarjeta de crédito para comprar en línea; muchas ofrecen protección y pueden reembolsarle el dinero.**
- **Desconfíe de los sitios web con errores ortográficos o gramaticales.**
- **Lea las políticas de reembolso y devolución con cuidado, incluyendo la letra pequeña.**
- **Haga preguntas al vendedor y confirme los tiempos de envío y el costo total.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

ESTAFAS DE VENTA DE PRODUCTOS

Los estafadores pueden presentarse como compradores.

Si usted vende artículos en línea, tanto personalmente como dentro de un negocio, debe tener cuidado con las personas a las que vende, ya que existe el riesgo de convertirse en el objetivo de estafadores que quieren quedarse con su mercancía, con su dinero, o ambos.

En algunos casos, el estafador acordará comprar sus productos sin verlos. Usted recibirá una notificación de PayPal o por correo electrónico indicando que el pago está pendiente.

El truco es que en la notificación le dirá que el pago solo se procesará cuando usted proporcione un número de seguimiento de los productos. En el momento en el que introduzca el número de seguimiento, ya habrá enviado la mercancía, y solo entonces descubrirá que la notificación de pago era falsa.

En otros casos, puede recibir una transferencia bancaria falsa, un cheque fraudulento o una tarjeta de crédito robada.

En otra versión de este fraude, el estafador puede enviarle un mensaje diciendo que no puede enviarse el pago debido a un problema con su cuenta bancaria o de PayPal. Se le pedirá que pague una tarifa para obtener una cuenta de negocios para completar la transacción. El estafador se ofrece a pagar la tarifa si usted le reembolsa utilizando un servicio de transferencias o financiero. Si acepta, el dinero para la "tarifa" irá directamente al estafador.

Consejos para protegerse:

- **Reúnase siempre en lugares locales, públicos y seguros para llevar a cabo un intercambio.**
- **Desconfíe de los correos electrónicos genéricos con faltas de ortografía.**
- **Desconfíe de los compradores de lugares lejos que quieren comprar productos u otros objetos sin verlos.**
- **Verifique la dirección de correo electrónico del remitente: los estafadores a menudo crean direcciones que son muy similares a las auténticas, con tan solo una o dos letras de diferencia.**
- **Nunca envíe dinero para recibir dinero.**

Si sospecha de una estafa, denúnciela siempre.

Vea las páginas 19 y 20 para obtener más información.

SEÑALES DE ALERTA: COSAS QUE VIGILAR

Aprenda a reconocer los signos de que algo falla.

Transferencia bancaria electrónica. Muchas estafas implican una petición de enviar dinero electrónicamente utilizando un servicio de transferencia de dinero como MoneyGram y Western Union, o utilizando criptomonedas como Bitcoin. Recuerde que realizar una transferencia mediante estos servicios es como enviar dinero en metálico: una vez que el envío haya sido recibido, será casi imposible recuperar su dinero.

Sobrepago. Cuando venda algo, sobre todo si lo hace por Internet, vigile el método de pago. Un estafador podría enviarle un cheque certificado, personal o comercial falso, por un importe superior a la cantidad que le debe. Se le pedirá que deposite el cheque y envíe inmediatamente la cantidad sobrante de vuelta. Cuando el banco descubra que el cheque es falso, usted ya habrá sido estafado con el dinero retirado.

Faltas de ortografía. Desconfíe de correos, mensajes o sitios web que contengan palabras comunes mal escritas; errores gramaticales que dificulten la lectura o expresiones utilizadas incorrectamente. Las direcciones de correo electrónico y de las páginas web deben ser también examinadas con cuidado para descubrir si hay pequeños errores o diferencias.

Peticiones de información personal. Los estafadores podrían solicitar a las potenciales víctimas que proporcionen más información personal o financiera de la requerida para la transacción o discusión. Sospeche si alguien le pide una copia de su pasaporte, licencia de conducir y número de seguridad social, o su fecha de nacimiento, especialmente si no conoce a quien se lo pide.

Llamadas no deseadas. Puede que reciba una llamada de alguien informándole de que tiene un virus en su ordenador, de que debe impuestos o que ha habido actividad fraudulenta en sus cuentas bancarias. Recuerde que las organizaciones legítimas no le llamarán directamente. Cuelgue y llame usted mismo a la organización utilizando el número de una fuente fiable, como la guía telefónica, su página web o incluso las facturas y extractos bancarios.

Solicitudes de amistad no deseadas en redes sociales. No acepte solicitudes de amistad de personas a las que no conoce hasta que no revise su perfil o pregunte a sus amigos de la vida real si conocen a esas personas. ¿Su perfil parece demasiado vacío o contiene entradas demasiado genéricas? ¿Parece estar prometiendo más que una amistad? Estas son algunas señales de alerta que indican que se trata de una estafa. Elimine la solicitud y bloquee futuras peticiones.

Ofertas increíbles por correo. Usted ha recibido una carta de un concurso por correo. Le garantiza que usted ganará o que ya ha ganado. Los premios pueden ir desde coches a viajes. Si no ha participado en un concurso, tire esa carta. ¡Probablemente sea un fraude!

Demasiado bueno para ser verdad. A todo el mundo le gustan las buenas ofertas. Pero las ofertas sorprendentes, los descuentos y precios increíbles pueden indicar que la oferta no es lo que parece. Los precios bajos suelen equivaler a productos de baja calidad, o productos falsificados. Las ofertas gratuitas pueden pedirle que proporcione su tarjeta de crédito para el costo del envío. Pequeñas tácticas como esta pueden dar lugar a grandes beneficios para los estafadores.

DENUNCIAR UNA ESTAFA

En función de dónde viva y del tipo de estafa que haya sufrido, deberá contactar a un determinado organismo.

Tanto si ha sufrido una estafa como si ha sido objetivo de un estafador, siempre debería denunciarlo. Es posible que las autoridades canadienses no siempre puedan tomar medidas contra las estafas, pero hay maneras de ayudar. Al denunciar la estafa, las autoridades podrán advertir a otras personas y alertar a los medios para que minimicen las posibilidades de que la estafa se extienda. También debería avisar a sus amigos y familiares de cualquier estafa con la que se haya encontrado.

A continuación se presentan algunos consejos sobre dónde denunciar, en función del tipo de estafa:

Canadian Anti-Fraud Centre (Centro Canadiense de Lucha contra el Fraude)
www.antifraudcentre.ca
1-888-495-8501

Competition Bureau (Oficina de la Competencia)
www.competitionbureau.gc.ca
1-800-348-5358

Estafas locales

Contacte a su oficina local de defensa de los consumidores

Su oficina local de defensa de los consumidores es el mejor recurso para investigar las estafas que parecen provenir de su propia provincia o territorio. Puede encontrar una lista de oficinas provinciales y territoriales de defensa de los consumidores en el Canadian Consumer Handbook (Manual del Consumidor Canadiense).

www.consumerhandbook.ca

Estafas financieras y de inversión

Contacte a Canadian Securities Administrators (Autoridades Canadienses de Valores Mobiliarios)

Las estafas financieras implican ofertas de ventas o promociones para productos y servicios financieros, como pensiones de jubilación, fondos gestionados, asesoría financiera, seguros, cuentas de crédito o depósitos.

Las estafas de inversión implican compras de acciones, compraventa de divisas, inversiones en el extranjero, esquemas piramidales (esquemas de Ponzi) o sistemas de inversión de “banco de primera” (*prime bank*).

Puede denunciar las estafas financieras y de inversión ante el Canadian Securities Administrators o ante su regulador de valores local.

www.securities-administrators.ca

Estafas bancarias y de tarjetas de crédito

Contacte a su banco o institución financiera

Además de denunciar estas estafas ante el Canadian Anti-Fraud Centre, debería alertar a su banco o institución financiera de cualquier correspondencia sospechosa que haya recibido en relación con su cuenta. Ellos podrán aconsejarle sobre cómo actuar.

Cuando contacte a su banco o institución financiera, asegúrese de usar el número de teléfono que aparece en la guía telefónica, en su extracto bancario o en el dorso de su tarjeta.

Correos electrónicos y mensajes de texto no deseados (*spam*)

Contacte al Spam Reporting Centre (Centro de Notificación de Spam)

Muchas estafas llegan a través del correo electrónico y los mensajes de texto. Visite www.fightspam.gc.ca para obtener información sobre la legislación contra el correo no deseado de Canadá y cómo denunciarlo.

Los mensajes fraudulentos, el *phishing* o el *smishing* en los que se solicitan datos personales también pueden denunciarse al banco, la institución financiera u otra organización pertinente. De nuevo, asegúrese de utilizar un número de teléfono o una dirección de correo electrónico que aparezca en una fuente oficial fiable, y no la que aparece en el correo recibido.

Fraude, robo y otros delitos

Contacte a la policía

Muchas estafas pueden suponer una violación de las leyes de protección de los consumidores (aquellas dictadas por el Competition Bureau y otras agencias del gobierno y los organismos policiales), y también pueden infringir las disposiciones antifraude del *Código Penal*.

Si usted ha sido víctima de un fraude (es decir, si ha sufrido una pérdida a causa del engaño o de la actuación deshonesta de alguien) considere contactar a su policía local, sobre todo si la cantidad en cuestión es significativa. Indudablemente, debe contactar a la policía si alguien ha robado su propiedad o sus bienes o si ha sido amenazado o agredido por un estafador.

Robo de identidad

Contacte a la policía

El robo de identidad se refiere a la adquisición y recopilación de la información personal de otra persona con fines delictivos.

Si sospecha o sabe que ha sido víctima de un robo o suplantación de identidad, o si proporcionó información personal o financiera involuntariamente, debería:

- Contactar a su policía local y presentar una denuncia.
- Contactar a su banco o institución financiera y a su compañía de tarjetas de crédito.
- Contactar a las dos oficinas nacionales de crédito y poner una alerta de fraude en sus informes de crédito.
- Denuncie siempre el robo de identidad y la suplantación. Contacte con el Canadian Anti-Fraud Centre.

Otras organizaciones a las que contactar dependiendo de la situación

- Su Better Business Bureau provincial
- Canada Revenue Agency—Charities Inquiries Line (Línea de consulta sobre las organizaciones benéficas)

  www.cra-arc.gc.ca
  1-800-267-2384
- Su oficina provincial de registros
- Las oficinas de crédito pueden poner un aviso de fraude en su cuenta, lo que alertará a los prestamistas y acreedores en caso de fraude potencial:

  Equifax Canada
  1-800-465-7166

  TransUnion Canada
  1-866-525-0262

El pequeño libro negro de las estafas está disponible en línea en www.competitionbureau.gc.ca

¡El conocimiento es poder!