



Saber un poco ahorra muchos problemas

Comercio electrónico

Conoce a tu proveedor en línea.

Cuando realices operaciones comerciales en línea, ten en cuenta los siguientes aspectos. ¡Es muy fácil verificarlos y tú tendrás la seguridad de estar tomando las precauciones necesarias para evitar ser víctima de prácticas comerciales fraudulentas!

- El proveedor debe informar claramente su identidad, denominación legal y datos de ubicación física tales como su dirección, teléfono y fax para que puedas hacer alguna reclamación en caso de que se presente un problema. También es importante el nombre o marca de comercialización de la empresa y sus productos.
- El proveedor de bienes y servicios por Internet está obligado a brindar al ciberconsumidor una descripción veraz de las características de los productos a fin de que el consumidor pueda tomar una decisión de compra bien informada.
En cuanto a los precios, recuerda que éstos deben estar expresados en moneda nacional y, en caso de existir cargos adicionales por envío de los productos, éstos deben señalarse claramente. Las condiciones y formas de pago también deben especificarse.
- Es deseable que el portal en el que estés realizando tus compras cuente con políticas de privacidad, sobre todo cuando la transacción implica que tú des a conocer algunos datos de carácter privado como el número de tu tarjeta de crédito.
- Es importante que el portal especifique, de manera clara, cuáles son las políticas de devolución de mercancías así como las garantías, las condiciones generales de la transacción, restricciones para la compra de bienes y servicios como es el caso de ubicación geográfica, de tiempo, por tipo de producto o cantidad a adquirir.

No dudes en verificar que el sitio en que pretendas comprar te ofrezca información clara sobre todas estas cuestiones.

Ley Federal de Protección al Consumidor

Cuando haces compras de forma tradicional, la ley te protege. De igual forma, en tus transacciones comerciales electrónicas también estás protegido. ¿Sabías que la Ley Federal de Protección al Consumidor contiene disposiciones sobre comercio electrónico? En el año 2000, se hicieron algunas reformas al texto de la ley para introducir el capítulo VIII Bis.

CAPÍTULO VIII BIS DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVÉS DEL USO DE MEDIOS ELECTRÓNICOS, ÓPTICOS O DE CUALQUIER OTRA TECNOLOGÍA

- " ARTICULO 76 bis.- Las disposiciones del presente capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
- I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.
- II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
- III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

- IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley demás disposiciones que deriven de ella;
- V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, (en su caso), y formas de pago de los bienes y servicios ofrecidos por el proveedor;
- VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
- VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población".

Lineamientos internacionales

Esta sección aborda las recomendaciones del Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) encaminadas a lograr la protección del consumidor en el contexto del comercio electrónico así como a evitar las prácticas comerciales transfronterizas fraudulentas y engañosas.

La Procuraduría Federal del Consumidor (Profeco) forma parte del Comité de Políticas del Consumidor (CCP) de la OCDE. Al interior de este Comité, se analizan las tendencias de las prácticas comerciales internacionales y se adoptan medidas de carácter general y que apelan a la cooperación internacional, a fin de evitar el comportamiento comercial abusivo que daña los intereses de los consumidores.

Así, en 1999, los países miembros del CCP de la OCDE, entre ellos México, adoptaron el texto de las [Directrices para la Protección de los Consumidores en el Contexto del Comercio Electrónico](#). Dicho documento contiene una serie de recomendaciones a los Estados miembros a fin de lograr que los proveedores de bienes y servicios a través de la Internet cumplan con las disposiciones de las leyes de protección al consumidor y garantizar con ello que el ciberconsumidor reciba el mismo nivel de protección cuando realiza sus transacciones comerciales "en línea" al igual que en la vía tradicional.

Posteriormente, en el año 2003, los miembros del CCP adoptaron las [Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas, Fraudulentas y Engañosas](#). Este documento hace un reconocimiento de que tales prácticas dañan la integridad de los mercados nacionales y globales en detrimento de todos los proveedores y consumidores y por ello efectúa una serie de recomendaciones a fin de que los Estados miembros puedan adoptar medidas que combatan tales comportamientos fraudulentos.

Cabe resaltar que ambas Directrices buscan generar la confianza del consumidor en el contexto del comercio electrónico.

Tendencias del comercio electrónico

Desde la publicación de los Lineamientos de Protección al Consumidor en el contexto del Comercio Electrónico de la Organización para la Cooperación y Desarrollo Económicos (OCDE) ha habido una evolución en las transacciones de los consumidores en el mercado en línea.

La estadística permite advertir el constante crecimiento de las ventas en línea al menudeo. Por ejemplo, las estadísticas oficiales del segundo trimestre de 2002 de las ventas al menudeo en el comercio electrónico en Estados Unidos de América (EUA) se incrementaron en un 24% comparado con el mismo período del 2001 y las estadísticas del 2001 fueron un 30% más elevadas que en el año 2000. Las ventas al menudeo en Internet del 2001 en Noruega fueron 155% mayores que en el 2000 y en Canadá se dio un crecimiento anual del 67% en 2001. Las estadísticas extraoficiales del gasto de los consumidores europeos en línea crecieron en un 48% en 2001 y un 70% en el 2000.

Estos niveles de crecimiento de las transacciones electrónicas no son iguales en todas las regiones del mundo. Así por ejemplo, de conformidad con el Informe de Comercio Electrónico 2003 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, por sus siglas en inglés), el comercio electrónico es una actividad que se concentra en un 95% en EUA, Reino Unido de la Gran Bretaña y los

países nórdicos. Por otra parte, África y América Latina representan menos del uno por ciento del total de transacciones electrónicas. En América Latina, este volumen procede principalmente de Brasil, México y Argentina.

No obstante, el potencial de las transacciones en línea aún está por alcanzarse. Ello se debe a que los consumidores siguen desconfiando del comercio electrónico.

Las compras individuales por Internet, a pesar de la proliferación de las tiendas "en línea" tampoco son representativas en México. Esta forma de consumo está concentrada en los países nórdicos, en Reino Unido de la Gran Bretaña y en EUA. Por su parte, Brasil tiene el mercado más maduro para el comercio minorista en América Latina toda vez que representa entre el 50 y 60 por ciento de las compras en línea.

En enero de 2002, la Red de Vigilancia del Consumidor (Consumer WebWatch) reportó que sólo tres de diez consumidores confían en los sitios web que venden productos o servicios. En julio de 2001, la Fundación Markle realizó un estudio el cual reportó que sólo el 36% de los individuos creen que tienen los mismos derechos y protección cuando realizan compras en Internet, como cuando los hacen por la vía tradicional. Una investigación dirigida por Consumers International (CI) sugiere que estas preocupaciones surgen cuando los consumidores enfrentan problemas con la entrega de los bienes, al realizar un pedido, así como la falta de reembolsos.

Lo anterior ha provocado que los ciber-consumidores presenten sus quejas a las agencias gubernamentales de protección al consumidor. En 2001, las quejas de los consumidores en torno de los problemas en línea sumaron un 41% de todas las quejas recibidas en el Consumer Sentinel, una base de datos (de quejas) que opera de manera conjunta en EUA y Canadá. El porcentaje de las quejas relacionadas con Internet en el Consumer Sentinel han aumentado firmemente: de un 11% en 1998, a un 26% en 1999, a un 31% en el 2000 y a un 41% en el 2001.

La desconfianza del consumidor es aún mayor en el contexto transfronterizo. Sólo el 32% de los consumidores europeos se sienten bien protegidos en una disputa transfronteriza, comparado con un 56 por ciento en una disputa doméstica. Un estudio de consumidores británicos reveló que más de un 60% no se involucraría en el comercio electrónico transfronterizo con una compañía que no conozca.

Las principales áreas problemáticas identificadas en las quejas incluyen que la mercancía nunca se recibe, información falsa de los bienes o servicios y la falta de disponibilidad para contactar al proveedor. El número de quejas transfronterizas también está incrementando.

Tomar ventajas completas de las promesas del mercado digital, requiere un mayor nivel de confianza por parte de los consumidores y los proveedores más exitosos serán aquellos que puedan demostrar su preocupación por reforzar la confianza de sus clientes.

Si quieres conocer más sobre tendencias de quejas de los ciber-consumidores, visita la [dirección electrónica](#).

Conceptos básicos

Cookies

Son programas que la mayoría de las veces las cookies son impuestas en el navegador sin su autorización, añadiendo pantallas aunque uno no lo desee. Su principal objetivo es identificar a los usuarios con el propósito de ajustar y personalizar una página web. Algunos sitios almacenan estas cookies en su navegador para que puedan ser utilizadas cuando se ingrese a la misma página nuevamente. El navegador buscará las cookies en la máquina y personalizará la página para usted. Actualmente existen programas para controlarlas, por lo que se recomienda instalar alguno de éstos, así como borrar periódicamente los archivos temporales de Internet.

Firewalls

El uso de un firewall o "barreras personales" protege las computadoras de los ciber piratas y evita que programas no deseados ingresen al sistema. Estas barreras protegen el sistema mientras se está conectado a Internet. También protegen de cookies no deseadas, así como la instalación y/o ejecución de programas en la computadora sin conocimiento y autorización del usuario. Su uso es recomendado al ingresar y navegar por Internet.

Robo de identidad

El "robo" o "fraude de identidad" es un delito por medio del cual alguien obtiene y utiliza datos e información personal de un tercero de manera fraudulenta. Este peligro se incrementa en virtud de que cada vez es más la información personal que circula libremente en Internet. Se recomienda especial cuidado con la información bancaria y de cuentas de tarjetas de crédito, débito y departamentales, reforzando sus contraseñas, cambiándolas periódicamente, así como el monitoreo constante de las cuentas bancarias.

Mensajes instantáneos, cuartos de charla y archivos compartidos

Los chats o "cuartos de charla", los "mensajes instantáneos", así como la "archivos compartidos" son formas de comunicación a través de Internet que permiten el envío y consulta de información en tiempo real y que sólo requieren un navegador o programa. Ello supone el riesgo de que la computadora se encuentre accesible para cualquier persona en Internet. Al compartir archivos se debe tener cuidado, porque además de los riesgos mencionados, existe la posibilidad de incurrir en responsabilidad al violar los derechos de autor. Se recomienda mantener actualizado el programa antivirus, instalar alguna barrera o firewall para que sólo se permita el acceso a la información que se desea compartir y no a todos los archivos. Finalmente, es importante no revelar detalles o información personal en cuartos de charla.

Difamación por Internet

Debemos ser responsables por aquella información falsa o perjudicial que mencionemos o publiquemos en Internet sobre personas o compañías, puesto que ellos podrían emprender alguna acción legal.

Protección de niños en línea

Los sitios web enfocados a menores de 13 años deben, para su seguridad, contener la siguiente información:

- La manera cómo se utilizará la información que proporcione el menor.
- Cómo se manejará la información con respecto a terceras personas (comerciantes, publicistas, etc.).
- Los padres deberán revisar la política de privacidad de cualquier sitio dirigido a menores, misma que deberá estar disponible en éste.
- Decidir otorgar o no el consentimiento a recolectar información personal de sus niños.
- Los operadores del sitio deben obtener nuevamente el consentimiento de los padres cuando cambien sus políticas.
- A los padres se les aconseja revisar la información que reciban sus hijos menores a efecto de detectar aquella que sea dañina para ellos y tomar las medidas pertinentes para su protección.
- Los padres tienen la opción de adquirir programas a fin de evitar que sus hijos reciban información de páginas para mayores de edad.

Scams o fraudes cibernéticos

"Suena bien, pero es demasiado bueno para ser cierto" ¿Cuántas veces hemos pensado esto? Se han detectado una gran diversidad de fraudes en Internet. Los más comunes son:

- Oportunidades de negocios e inversión prometiendo grandes ingresos y/o ganancias sin mucho trabajo o a un bajo costo; la mayoría son esquemas piramidales ilícitos.
- Las famosas "cadenas" transmitidas a varias personas ofreciendo una pequeña cantidad de dinero a cambio de mandarlas a más personas.
- Esquemas y ofertas de trabajo en casa, en las que se prometen ingresos con el pago previo de una cantidad.
- Fraudes con dietas y servicios y/o cosmetológicos de salud en donde se ofrecen pastillas, fórmulas naturales, curas de impotencia, pérdida de cabello, etc.
- Regalos, con el previo pago de una cantidad para ingresar a algún grupo.

Acoso por Internet

Se presenta por medio de amenazas para perseguir a otra persona por Internet, ya sea por correos electrónicos o por mensajes en línea. Para evitarlo se recomienda borrar las identificaciones (antecedentes) que se hayan creado en cuartos de charla y sistemas de mensajes instantáneos, cambiar direcciones de correo electrónico o en caso de ser necesario, contactar a su proveedor de servicio de Internet.

Contraseñas

Los passwords o "contraseñas" son tan importantes como la llave de su casa. Los ciberpiratas o hackers son ladrones de contraseñas, por lo que es importante que éstas sean difíciles de descifrar. Una contraseña simple puede ser descubierta mediante un programa especializado en menos de una hora; en cambio una contraseña difícil puede tardar de 10 a 20 años en ser descubierta.

Toma en cuenta las siguientes recomendaciones:

- No utilizar como contraseña alguna palabra que se encuentre en un diccionario, incluso en cualquier idioma.
- No utilizar palabras al revés.
- No usar una palabra que pueda ser asociada con información personal, dirección, teléfono, fecha de nacimiento, nombre de la mascota, pasatiempo o deporte favorito.
- No utilizar letras o números consecutivos, por ejemplo "abcdefg" o "123456".
- Tratar que sea lo más simple a efecto de que se pueda recordar.
- Utilizar una combinación de letras, números y caracteres especiales en orden aleatorio.
- Utilizar por lo menos 6 caracteres. Cuanto más sean, más difícil será de descifrar.

Puntos de acceso público

Muchas personas no tienen la posibilidad de ingresar a Internet desde una computadora propia, o en caso de estar de viaje y requerir de Internet para mantenerse comunicado, se puede acudir a lugares o puntos de acceso público (café Internet, bibliotecas, librerías, aeropuertos, etc.). En estas circunstancias, también hay que tomar precauciones para cuidar la información personal y navegar de manera segura por la red. A continuación, algunas recomendaciones:

- Estar siempre alerta de las personas que se encuentren o estén sentadas cerca de ti, ya que podrían ver tu información personal en pantalla.
- Eliminar la memoria "temporal" del navegador antes de retirarte del lugar de la siguiente manera: desplegar el menú de herramientas, seleccionar opciones de Internet, dar un click en "eliminar archivos" y "borrar historial". Esto ayudará a minimizar el riesgo de que alguien tenga acceso a tu información personal.
- Cerrar todas las páginas utilizadas antes de dejar el lugar.
- Nunca permitir a la computadora recordar contraseñas.
- Nunca ingresar información privada o importante mientras te encuentras en un sitio de acceso público.

Spam

Junto con los "correos electrónicos chatarra" se trata de correos electrónicos no solicitados y enviados de manera masiva. El contenido de éstos se relaciona con publicidad de bienes y servicios; algunas compañías pagan por enviar publicidad y circulares. Varios usuarios pagan el servicio de Internet por horas y es obvio que invertirán más tiempo al abrir estos correos, que pueden llegar a saturar los buzones. Por lo general, el spam es retransmitido de forma indiscriminada, anónima, encubierta y repetitiva. Además, las personas que envían spam (spammers) utilizan direcciones electrónicas que fueron recolectadas o vendidas sin previo consentimiento del usuario.

Se recomienda tener las siguientes precauciones para evitar este tipo de correo:

- Nunca responder a un correo spam, de lo contrario se confirmaría la dirección y sería un objetivo idóneo para futuros correos.
- No utilizar la cuenta de correo normal o privada para suscripciones, listas de correo o publicidad. Se recomienda crear una cuenta especial para estos fines.
- Nunca comprar algo que se anuncie a través de correos spam.

- Utilizar un filtro especial para estos correos. Generalmente, los servicios de correo cuentan con tal opción.
- Reportar a las empresas spammers en los sitios denominados antispam.
- Revisar detenidamente las políticas de privacidad al momento de abrir una cuenta de correo.
- No abrir los archivos anexos a correos spam.

Spyware y "Caballos de Troya"

Debemos tener cuidado con los programas ejecutables (aquellos que puedes recibir a través de correos electrónicos y cuya terminación es ".exe") ya que existen algunos que utilizan tu computadora y realizan conexiones automáticas a otros sitios, enviando tu información personal sin autorización y sin conocimiento de ello. Los programas "trojanos" permiten a un ciber pirata acceder a toda tu computadora y manejar tu información personal. Es recomendable tomar precauciones, como revisar la configuración de "cookies" e instalar "barreras". También existen programas para detectar a los espías y ciber piratas.

Virus

Son programas cuyo objetivo es destruir o dañar archivos. Son transmitidos de computadora en computadora. Para evitar una infección es recomendable:

- Tener la versión más actualizada de antivirus y actualizarlo constantemente.
- Nunca abrir un correo electrónico desconocido o inesperado.
- Revisar todos los archivos contenidos en correos electrónicos antes de descargarlos, aún los de tus amigos o conocidos.

Recomendaciones generales

El Internet es un espacio del que puedes obtener diversos beneficios si tomas en cuenta algunas precauciones. No importa si eres niño, adolescente, un adulto joven o uno mayor, lo importante es que sigas algunos simples consejos a fin de tratar de disminuir los riesgos en la Red.

Cabe señalar que Profeco ha estado trabajando en estrecha colaboración con el Grupo Delitos Cibernéticos México, a través del subgrupo de Valores, políticas de uso y regulación de Internet, del que esta institución forma parte. Dicho Grupo ofrece recomendaciones a los niños usuarios de Internet para navegar en forma segura. Se trata de un esfuerzo coordinado por orientar a los usuarios de Internet sobre los niveles de inseguridad y de intrusión a la privacidad de su información durante la conexión a Internet.

Recuerda: Internet puede ser un buen aliado de todos, conociendo algunos sencillos Tips de Seguridad.

- [Recomendaciones generales](#)
- [Recomendaciones para niños](#)
- [Recomendaciones para padres](#)

Recomendaciones generales

Al navegar en Internet es importante tomar en cuenta las siguientes sugerencias:

- Buscar y leer las políticas de privacidad de información personal de cada sitio antes de efectuar alguna operación o registro.
- Verificar que las formas de registro en línea sean seguras.
- Rechazar las cookies innecesarias.
- Utilizar un buscador o navegador y asegurarse de que sea la última versión disponible por el proveedor.
- No proveer más información personal que la necesaria para completar alguna operación o registro, a menos que te sientas seguro con las políticas del sitio y que tu información será transmitida a través de un vínculo seguro.
- Nunca divulgar tu contraseña en línea o por teléfono.
- Controlar las cookies. Descarga un programa para ello. Revisa las propiedades de seguridad en las opciones de Internet y ajústalas según sus necesidades.
- Eliminar de manera regular los archivos temporales de Internet.

- Instalar y utilizar una "barrera de acceso".
- Disponer de la versión más reciente de antivirus y actualizar ce periódicamente su programa antivirus.
- Nunca abrir o descargar archivos desconocidos contenidos en correos electrónicos o de procedencia sospechosa.
- Tener cuidado al instalar algún programa descargado vía Internet, al igual que cuando se comparte información o se permite el acceso a los archivos, o al instalar programas de charla en línea, mensajes instantáneos, etc.
- Informarse de los derechos de autor y consecuencias legales que pueda traer consigo el compartir archivos.
- No revelar detalles personales en charlas en línea.
- Estar consciente de que en Internet no todo es totalmente confiable.
- Nunca contestar un correo spam. Al hacerlo, se confirmará la dirección electrónica y será un blanco perfecto para este tipo de correos.
- No utilizar la cuenta de correo normal para suscripciones, listas, páginas, etc. En otras palabras, mantener una dirección privada y una pública.
- Se recomienda utilizar un filtro para los correos spam.
- Crear un pasaporte seguro para comprar más fácilmente cuando se navega en los diferentes sitios. Visitar <http://www.passport.com>.
- Existen sitios que en su dirección se observa https en lugar del http habitual. Esto quiere decir que el sitio fue creado de conformidad con la legislación aplicable al país. Es necesario buscar en la pantalla un candado o llave, que son indicaciones de que el sitio utiliza tecnología especial para proteger los números de las tarjetas de crédito, así como la información transmitida.
- Crear contraseñas para las cuentas de compras en línea utilizando 6 o más letras mayúsculas y minúsculas, números y otros símbolos escogidos aleatoriamente.
- No utilizar la misma contraseña para más de un sitio o cuenta.
- Entender claramente las políticas de privacidad; poner especial atención en aquellas cláusulas que mencionen las operaciones de envío, cancelaciones y devoluciones de los productos ofrecidos en el sitio.
- En caso de que exista una sección faq (frequently ask question o preguntas frecuentes) es recomendable leerla para saber más sobre ese sitio.
- Mantener registro de todas las transacciones en línea. Podrías necesitar esa información para realizar aclaraciones sobre algún cargo a tu tarjeta no autorizado.
- Revisar mensualmente los estados de cuenta de tu tarjeta para asegurarte de que no existan cobros indebidos. En caso de que así sea, denuncia el hecho a la [Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros \(CONDUSEF\)](#).
- Cuidarse de las compañías que hacen ofertas difíciles de creer o casi imposibles; puede tratarse de un negocio poco serio.
- Conocer a la compañía con que trata. Los proveedores honestos proporcionan instrucciones e información clara sobre su negocio y resolverán tus sus dudas en el momento en que lo solicites.
- Obtener números telefónicos y domicilios físicos de los proveedores en línea antes de proporcionarles la información personal.

Al navegar en Internet es importante tomar en cuenta las siguientes sugerencias:

- Buscar y leer las políticas de privacidad de información personal de cada sitio antes de efectuar alguna operación o registro.
- Verificar que las formas de registro en línea sean seguras.
- Rechazar las cookies innecesarias.
- Utilizar un buscador o navegador y asegurarse de que sea la última versión disponible por el proveedor.
- No proveer más información personal que la necesaria para completar alguna operación o registro, a menos que te sientas seguro con las políticas del sitio y que tu información será transmitida a través de un vínculo seguro.
- Nunca divulgar tu contraseña en línea o por teléfono.
- Controlar las cookies. Descarga un programa para ello. Revisa las propiedades de seguridad en las opciones de Internet y ajústalas según sus necesidades.
- Eliminar de manera regular los archivos temporales de Internet.
- Instalar y utilizar una "barrera de acceso".
- Disponer de la versión más reciente de antivirus y actualizar ce periódicamente su programa antivirus.

- Nunca abrir o descargar archivos desconocidos contenidos en correos electrónicos o de procedencia sospechosa.
- Tener cuidado al instalar algún programa descargado vía Internet, al igual que cuando se comparte información o se permite el acceso a los archivos, o al instalar programas de charla en línea, mensajes instantáneos, etc.
- Informarse de los derechos de autor y consecuencias legales que pueda traer consigo el compartir archivos.
- No revelar detalles personales en charlas en línea.
- Estar consciente de que en Internet no todo es totalmente confiable.
- Nunca contestar un correo spam. Al hacerlo, se confirmará la dirección electrónica y será un blanco perfecto para este tipo de correos.
- No utilizar la cuenta de correo normal para suscripciones, listas, páginas, etc. En otras palabras, mantener una dirección privada y una pública.
- Se recomienda utilizar un filtro para los correos spam.
- Crear un pasaporte seguro para comprar más fácilmente cuando se navega en los diferentes sitios. Visitar <http://www.passport.com>.
- Existen sitios que en su dirección se observa https en lugar del http habitual. Esto quiere decir que el sitio fue creado de conformidad con la legislación aplicable al país. Es necesario buscar en la pantalla un candado o llave, que son indicaciones de que el sitio utiliza tecnología especial para proteger los números de las tarjetas de crédito, así como la información transmitida.
- Crear contraseñas para las cuentas de compras en línea utilizando 6 o más letras mayúsculas y minúsculas, números y otros símbolos escogidos aleatoriamente.
- No utilizar la misma contraseña para más de un sitio o cuenta.
- Entender claramente las políticas de privacidad; poner especial atención en aquellas cláusulas que mencionen las operaciones de envío, cancelaciones y devoluciones de los productos ofrecidos en el sitio.
- En caso de que exista una sección faq (frequently ask question o preguntas frecuentes) es recomendable leerla para saber más sobre ese sitio.
- Mantener registro de todas las transacciones en línea. Podrías necesitar esa información para realizar aclaraciones sobre algún cargo a tu tarjeta no autorizado.
- Revisar mensualmente los estados de cuenta de tu tarjeta para asegurarte de que no existan cobros indebidos. En caso de que así sea, denuncia el hecho a la [Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros \(CONDUSEF\)](#).
- Cuidarse de las compañías que hacen ofertas difíciles de creer o casi imposibles; puede tratarse de un negocio poco serio.
- Conocer a la compañía con que trata. Los proveedores honestos proporcionan instrucciones e información clara sobre su negocio y resolverán tus sus dudas en el momento en que lo solicites.
- Obtener números telefónicos y domicilios físicos de los proveedores en línea antes de proporcionarles la información personal.

Recomendaciones de seguridad para menores que navegen en internet

- Platica siempre con tus padres o un adulto de tu confianza sobre las personas que contactas en Internet.
- No confíes en todo lo que te cuentan las personas que conoces en chats o canales de plática, puede ser que no tengan buenas intenciones contigo e inventen situaciones que no son reales para llamar tu atención.
- Consulta con tus padres primero o una persona adulta de tu confianza, si puedes proporcionar datos a un amigo o conocido en Internet.
- Nunca le mandes tu foto a un "amigo virtual" que te la solicite en Internet.
- Pon atención a lo que ves en Internet, ya que no todo lo que hay en el medio es real, muchas cosas solo existen en la realidad virtual que se crea en Internet.
- Desconfía siempre de las invitaciones y promociones "demasiado buenas para ser verdad" que te ofrecen.
- Si alguien en Internet te molesta, atemoriza, o te hace sentir incómodo, díselo a tus padres o a un adulto de tu confianza, y denúncialo a la policía cibernética de la PFP, al teléfono 01 800 440 36 90 ó 52 41 04 20 / 52 41 04 21 ó al correo electrónico policia_cibernetica@ssp.gob.mx

Recomendaciones de seguridad para padres relacionados con el usos de internet

- Procure que la computadora en casa esté en un sitio visible, y no en las recámaras o cuartos cerrados o aislados de la casa, esto permitirá la fácil y constante supervisión de lo que ven o buscan los niños y jóvenes en Internet.
- Infórmese sobre programas especializados de filtro y/o bloqueo que evitan que los niños y jóvenes tengan acceso a sitios nocivos para su salud física y mental. Algunos de éstos se obtienen gratis de Internet y otros se pueden comprar con proveedores de este tipo de servicios.
- Explique a los niños y jóvenes que no todo lo que se ve en Internet es real, ya que mucho de su contenido es virtual y algunos contenidos son peligrosos. Hágales saber que pueden recurrir a un adulto cuando se encuentren con información inconveniente.
- Pase algún tiempo con sus hijos mientras navegan en Internet y muestre interés por las personas con las que se comunica, al igual como lo hace con sus amigos reales. Hable con los padres de los amigos de sus hijos y trabajen en conjunto para ofrecer un ambiente de navegación seguro.
- Advierta a los niños y jóvenes que no deben confiar en cualquier persona que se encuentren en chats y/o canales de plática, ni proporcionar sus datos personales o citarse con extraños sin su autorización que pudiera poner en riesgo la seguridad de la familia. No deben compartir nunca fotos de ellos o de la familia con personas que conocen en Internet.
- Proteja las contraseñas de sus hijos y cree nombres genéricos. Asegúrese de que sus hijos no tengan alias que revelen su información personal, incluyendo su nombre completo, edad, género, etc.
- Rechace el spam (Correo Electrónico no deseado). Instale software de filtrado de spam, para evitar que sus hijos reciban correo electrónico ofensivo.
- Advierta que no deben llenar cuestionarios que se encuentren en Internet sin su permiso y supervisión.
- Enseñe a no aceptar dinero o favores de extraños.
- Enseñe a sus niños a velar por su propia seguridad. Advértales que nunca revelen la contraseña de Internet a ninguna persona incluso si esa persona dice trabajar para un proveedor de servicio de Internet.
- Limite el tiempo que los niños y jóvenes usan para navegar en Internet.
- No proporcione a sus hijos los números de tarjetas de crédito que manejan.
- Si detecta una página, sitio, comunidad o persona en chat que promueva, distribuya, produzca y/o venda pornografía infantil en Internet denúnciela a la policía cibernética de la PFP a los teléfonos 01 800 440 36 90 ó 52 41 04 20 / 52 41 04 21 ó al correo electrónico policia_cibernetica@ssp.gob.mx

Si toma estas medidas sencillas y mantiene una comunicación abierta con sus hijos sobre los parámetros para el uso de Internet, se puede sentir tranquilo al permitirles tener una experiencia educativa y segura en línea cada vez que naveguen.

Alerta al consumidor

Profeco vigila permanentemente prácticas comerciales indebidas y publicidad engañosa; inmoviliza productos peligrosos e impone multas y clausuras a las empresas que atentan contra los derechos de los consumidores. Usted, por su parte, tiene el poder: el poder de no comprar y de presentar una queja o denuncia.

Si conoce algún caso de abuso al consumidor, háganoslo saber al teléfono 01-800-468-8722 Profeco pone la alerta.

- [Riesgos de adquirir juguetes réplica de armas](#)
17de diciembre de 2004
- [Llamadas telefónicas que tratan de engañarlo](#)
17de diciembre de 2004
- [Publicidad de boletos de avión](#)
17de diciembre de 2004
- [Correos electrónicos engañosos](#)
17de diciembre de 2004
- ["Certificado por Notario Público"](#)
17de diciembre de 2004
- [Incendios en navidad](#)
1° de diciembre de 2004

- [Aliviar no significa curar](#)
1º de diciembre de 2004
- [Alto riesgo en internet](#)
1º de diciembre de 2004
- [Falso tequila de Tequila, las destilerías clandestinas](#)
1º de diciembre de 2004
- [Vioxx, peligro mortal que venden en las farmacias](#)
1º de diciembre de 2004
- [Las bebidas alcohólicas que venden en Tepito son falsificadas](#)
1º de noviembre de 2004

Preguntas más frecuentes

Subastas en línea

[Compré un artículo en una subasta por Internet. Cuando lo recibí no estaba en las condiciones descritas en el sitio electrónico y además le faltaban componentes. ¿Cuáles son mis derechos?](#)

Cuando compras bienes a través de una subasta por Internet, en términos generales, no estás comprando directamente de la casa de subastas, sino a un individuo o compañía que está utilizando los servicios de subasta. Como regla general, la casa de subastas no se responsabilizará por la condición en la que se encuentren los artículos. En este caso, deberás arreglarte con el individuo o compañía que te vendió el objeto. No obstante, por ley, un producto adquirido a través de una subasta de Internet debe estar en buenas condiciones (razonablemente buenas) y debe corresponder con la descripción que se ofreció del artículo. Si argumentas que la publicidad fue engañosa o que no se encuentra en las condiciones en las que fue descrito en la subasta puedes reclamar.

Tips para transacciones en sitios de subastas.

- Antes de ofrecer o comprar algo, lee a los términos y condiciones de la compañía de subastas en línea.
- Encuentra e los datos para localizar al proveedor de bienes o servicios.
- Averigua algo sobre la conducta previa del proveedor a través de los foros de re-alimentación que ofrecen algunas casas de subasta en línea.
- Para compras mayores, utiliza un servicio de agentes de retención de pago. Un servicio así consiste en que una tercera parte retiene el pago que efectúas por el bien o servicio hasta que el comprador recibe el bien y manifiesta su satisfacción.

Artículos dañados

[Compré un artículo en línea pero se dañó durante el envío por correo. ¿Qué puedo hacer?](#)

Primero contacta al proveedor a fin de revisar qué es lo que ellos pueden hacer en estos casos. Si el paquete se originó en México, tal vez quieras contactar también a las Oficinas del Servicio Postal Mexicano o a la compañía responsable de mensajería. Si el paquete se originó en el extranjero, tu queja deberá presentarse a quien envió el paquete. Como práctica generalizada, una vez que el objeto ha sido depositado en los servicios de mensajería, el comprador asume el riesgo. Así que asegura tu compra antes de que sea enviada.

Envíos

[Compré un artículo "en línea" a un precio de rebaja pero no me di cuenta que la cuota de envío sería casi el doble del precio del artículo. ¿Puedo regresar el artículo y obtener un reembolso por el precio del éste y por la cuota de envío?](#)

Los envíos pueden ser caros dependiendo de la ubicación de la compañía, así que ten cuidado cuando realices compras en línea de que la oferta de tu vida puede no ser en realidad una buena opción.

Un sitio de ventas por Internet que ejerce buenas prácticas de comercialización, debe señalar claramente a sus clientes cuáles son los cobros por envío. No informar al consumidor constituye una violación a los derechos de éste. Revisa las políticas en la página del sitio. Imprime toda la información relevante, tal como tu recibo y la confirmación de la orden. Finalmente, no entables negocios con una compañía que no te informe claramente la totalidad de los cargos.

Pagos

Compré un artículo en un portal. Contacté a un vendedor quien se comprometió a enviarme el artículo si le depositaba; efectué el depósito y es el día que no tengo noticias de esta persona, tengo su cuenta lo que quiere decir que el nombre es real, ¿qué puedo hacer?

Desafortunadamente, el número de la cuenta bancaria no te garantiza que estés tratando con una persona confiable. En ese sentido, intenta contactar una vez más al vendedor a través de su correo electrónico o bien llámalo por teléfono con objeto de exponerle el problema. Si no te contestan o no cuentas con estos datos, has sido defraudado. Por ello, denuncia a esta persona en Profeco. La Ley Federal de Protección al Consumidor (LFPC) te protege toda vez que el capítulo 76 bis establece que "el proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones ..."

Confiabilidad

¿Cómo puedo saber si una página de Internet que ofrece bienes y servicios es confiable?

Cada vez que realices una transacción en línea considera r los elementos básicos que una página de Internet debe contener:

1. Domicilio.
2. Denominación legal.
3. Nombre o marca de comercialización de la empresa y sus productos.
4. Número telefónico, fax para cualquier aclaración.
5. El producto debe ser claramente identificado y señalar sus características.
6. Condiciones y formas de pago, costos e impuestos.
7. Costos de envío y términos de entrega.
8. Política de garantía y reembolso.
9. Política de privacidad de datos.
10. Política de seguridad.
11. Restricciones para la adquisición de bienes y servicios ofrecidos, como geográfica, de tiempo, por tipo de producto o cantidad a adquirir.

Si la página no cuenta con estos elementos entonces no confíes en ella. Seguramente es un proveedor propenso a cometer prácticas comerciales desleales o abusivas.

¿Te incumplieron? ¿Quieres presentar una queja?

Si celebraste una operación comercial electrónica con un proveedor de bienes y servicios que se encuentra domiciliado en el extranjero, te tenemos una buena noticia, Profeco es parte del proyecto internacional eConsumer.gov, espacio en Internet para apoyarte en tu reclamación cuando un proveedor te haya incumplido con los términos de compra realizadas a través de comercio electrónico. Revisa el sitio, es una herramienta útil para ti.

Por otra parte, si tu problema es con un proveedor de bienes y servicios domiciliado en territorio nacional, [acércate a Profeco](http://Profeco). Nosotros te atendemos y asesoramos cuando celebres operaciones comerciales en línea.
