Prácticas abusivas en el comercio electrónico

PIENSA

Hoy ya no es necesario acudir a una tienda física o a una gran superficie para comprar productos o contratar servicios, todo esto lo puedes hacer desde tu casa o desde donde tú quieras, simplemente conectándote a la red.

A día de hoy, en la mayoría de los casos, las empresas tienen su punto de venta online. Incluso, muchas de ellas no tienen punto de venta física. Las tiendas online amplían la flexibilidad de las compras, puedes comprar durante las 24h del día cualquier día de la semana, lo que permite captar un número mayor de clientes. Pero también genera muchas emisiones de CO_2, muchos residuos, muchas compras compulsivas e innecesarias; sin menoscabo de otras circunstancias, pérdida del tejido comercial en los barrios, deslocalización de la producciones y de los intercambios comerciales, datos engañosos de productos y sitios web, uso de nuestros datos personales, etc.

SABÍAS QUE...

 Conlleva también algunos inconvenientes, como la imposibilidad de ver físicamente el producto, poder probarlo y estar seguro de que es realmente lo que queremos.

La primera recomendación a la hora de hacer una compra segura a través de Internet es estar bien informado: saber dónde y a quién se está comprando, es decir, quién está detrás de una página web de venta o prestación de servicio.

CONFIANZA EN EL SITIO WEB DONDE VAMOS A COMPRAR

Es necesario comprobar que la empresa esté suficientemente identificada: nombre o denominación social, dirección física y dirección de correo electrónico, teléfono, NIF, datos de inscripción en el registro mercantil… Estos deben aparecer obligatoriamente en la página web y, ante la duda, hay que evitar comprar en sitios donde no aparezca una dirección física o donde la única forma de contacto sea a través de un móvil. La LSSI (Ley de Servicios de la Sociedad de la Información) obliga a incluir todos estos datos en todas las páginas de comercio electrónico.

Además deberán ofrecer un enlace electrónico a la plataforma de Resolución de litigios en línea (ODR) (Reglamento UE 524/2013) y, en aquellos casos en los que las empresas se hayan comprometido a resolver los posibles conflictos que surjan durante la compra a través de entidades de resolución de conflictos, en el caso de España, a través de las Juntas Arbitrales de Consumo, proporcionaran el enlace electrónico a dichas entidades.

PAGO SEGURO

No siempre es necesario pagar con tarjeta. Existen diferentes métodos de pago para las transacciones online: tarjeta de crédito, pago contra-reembolso, ingresos/transferencias en cuenta, sistema de pago electrónico (tipo PayPal), pagos a través del móvil... Cada comercio incorpora los que cree convenientes.

Algunos bancos ofrecen un servicio de tarjeta virtual pensado únicamente para pagar en Internet. Lo llaman cybertarjeta, es gratuita y no hace falta dar los datos personales para obtenerla, con lo que se garantiza la privacidad y el anonimato.

Si vamos a introducir información personal y el número de nuestra tarjeta de crédito, tenemos que tener la certeza de que la transacción va a ser completamente segura. Para ello, debemos comprobar que:

La dirección web comience por HTTPS. Las direcciones web normalmente comienzan con HTTP. En cambio, las páginas creadas para realizar pagos, que tienen más seguridad, comienzan por HTTPS (viene de HTTP Seguro). A la derecha de la dirección web podremos también ver el icono de un candado, que aporta más información sobre la seguridad de la página. Es el llamado «certificado de seguridad».

Hay tiendas que ofrecen además un Sello de Confianza Online que pretende garantizar la confianza de los usuarios en Internet por medio de un distintivo (sello de Confianza Online).

Confianza Online es una asociación que dispone de un código de buenas prácticas, que se comprometen a firmar y respetar las empresas de Internet y comercio electrónico adheridas a ella.

Una tienda virtual también nos tiene que ofrecer una garantía clara sobre el producto que estamos comprando. En la página web tiene que aparecer información sobre: plazos de entrega, formas de pago, derecho al desistimiento de la compra sin que medie motivo, política de devolución, características del producto o servicio y garantías del mismo.

Una vez que ya se ha tomado la decisión de comprar, es necesario leer atentamente las condiciones generales del contrato ya que, cuando se marca una casilla aceptando las condiciones, es como si se firmara un contrato.

Lo más conveniente es hacer una lectura atenta e imprimir y guardar una copia. Antes de esto, sin embargo, se debe repasar el resumen de la compra, el precio total (con especial atención a los gastos de envío o a cualquier otro concepto que no venga especificado) y vigilar que los datos personales introducidos sean los estrictamente necesarios para la transacción. Con ello evitarás que pueda llegarte *spam* (correo basura) o llamadas telefónicas indeseadas.

Recuerda que a la hora de introducir tus datos en la web debes tener presente la política de privacidad del sitio. Las empresas están obligadas a informar sobre la finalidad de estos datos y tienen que dar la opción de corregirlos o cancelarlos. Tampoco pueden ceder esos datos a terceros sin tu consentimiento expreso. En

cualquier caso, esta política de privacidad debe estar claramente publicada en la web y todos los datos recogidos tienen que pasar por la Agencia Española de Protección de Datos.

Prácticas abusivas en el comercio electrónico.

Las **prácticas comerciales desleales, o abusivas**, son todo acto, conducta o manifestación comercial (incluida la publicidad y la comercialización) que un empresario realiza en su relación con los consumidores que sea objetivamente contrario a los requisitos de diligencia profesional y de buena fe. Esto incluye el comercio electrónico y físico.

Se incluyen en esta noción dos grandes tipos de prácticas que afectan al comportamiento y decisión de los consumidores a los que se dirigen, pudiendo provocar que éstos adopten decisiones de consumo que en condiciones adecuadas de información y claridad no habrían adoptado:

- Prácticas engañosas, ya sea por acción (dar información falsa) o por omisión (ocultar información importante).
- Prácticas agresivas para forzarte a comprar.

Tales prácticas comerciales son desleales “en todo caso y en cualquier circunstancia” y algunas de ellas son:

- **Prácticas engañosas sobre códigos de conducta u otros distintivos de calidad** como afirmar el empresario que está adherido a un código de conducta sin ser cierto o la exhibición de un sello de confianza o de calidad o de un distintivo equivalente, sin haber obtenido la necesaria autorización.
- **Prácticas señuelo y prácticas promocionales engañosas** como la denominada “oferta vacía” en la que el empresario, después de promocionar un bien o un servicio a un precio determinado, normalmente muy competitivo, con la finalidad de atraer a los consumidores, no dispone de las existencias suficientes para atender la demanda previsible; o aquélla consistente en ofrecer un premio a un consumidor de forma automática, si luego ese premio no se entrega.
- **Prácticas engañosas sobre la naturaleza y propiedades de los bienes o servicios**, su disponibilidad y los servicios posventa como proclamar falsamente que un bien o servicio puede curar enfermedades, disfunciones o

malformaciones.

- **Prácticas de venta piramidal** como crear, dirigir o promocionar un plan de venta piramidal en el que el consumidor o usuario realice una contraprestación a cambio de la oportunidad de recibir una compensación derivada fundamentalmente de la entrada de otros consumidores o usuarios en el plan, y no de la venta o suministro de bienes o servicios.
- **Prácticas engañosas por confusió**n como promocionar un bien o servicio similar al comercializado por un determinado empresario o profesional para inducir de manera deliberada al consumidor o usuario a creer que el bien o servicio procede de este empresario o profesional, no siendo cierto.
- **Prácticas comerciales encubiertas** como incluir información en los medios de comunicación para promocionar un bien o servicio, pagando el empresario por dicha promoción, sin que quede claramente especificado en el contenido o mediante imágenes y sonidos claramente identificables para el consumidor que se trata de un contenido publicitario.
- **Otras prácticas engañosas** como presentar los derechos que otorga la legislación a los consumidores o usuarios como si fueran una característica distintiva de la oferta del empresario o profesional; transmitir información inexacta o falsa sobre las condiciones de mercado o sobre la posibilidad de encontrar el bien o servicio, con la intención de inducir al consumidor o usuario a contratarlo en condiciones menos favorables que las condiciones normales de mercado.
- **Prácticas agresivas por coacción** como hacer creer al consumidor o usuario que no puede abandonar el establecimiento del empresario o el local hasta haber contratado, salvo que dicha conducta sea constitutiva de infracción penal.
- **Prácticas agresivas por acoso** como realizar visitas en persona al domicilio del consumidor o usuario, ignorando sus peticiones para que el empresario abandone su casa o no vuelva a personarse en ella.
- **Prácticas agresivas en relación con los menores**, prácticas publicitarias que tienen como objetivo que los menores convenzan a los adultos que les compren un determinado artículo o servicio.
- **Otras prácticas agresivas** como informar expresamente al consumidor o usuario de que el trabajo o el sustento del empresario o profesional corren peligro si el consumidor o usuario no contrata el bien o servicio.

Por su parte, y en relación con estas prácticas: las cláusulas abusivas son todas aquellas estipulaciones no negociadas individualmente, sino impuestas por el empresario sin que puedan ser discutidas, así como todas aquellas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe, causen, en perjuicio del consumidor y usuario, un desequilibrio importante en los derechos y obligaciones de las partes que se deriven del contrato:

- Las cláusulas abusivas de los contratos serán nulas de pleno derecho y se tendrán por no puestas.
- Sólo un juez puede declarar la nulidad de las cláusulas abusivas incluidas en el contrato, el cual seguirá siendo obligatorio para las partes siempre que pueda subsistir sin dichas clausulas. En todo caso serán cláusulas abusivas las que:

- Vinculen el contrato a la voluntad del empresario como aquellas que prevean la prórroga automática de un contrato de duración determinada si el consumidor y usuario no se manifiesta en contra, fijando una fecha límite que no permita de manera efectiva al consumidor y usuario manifestar su voluntad de no prorrogarlo.

- Limiten los derechos del consumidor y usuario como la exclusión o limitación de forma inadecuada de los derechos legales del consumidor y usuario por incumplimiento total o parcial o cumplimiento defectuoso del empresario

- Determinen la falta de reciprocidad en el contrato como la imposición de obligaciones al consumidor y usuario para el cumplimiento de todos sus deberes y contraprestaciones, aun cuando el empresario no hubiere cumplido los suyos o la retención de cantidades abonadas por el consumidor y usuario por renuncia, sin contemplar la indemnización por una cantidad equivalente si renuncia el empresario

- Impongan al consumidor y usuario garantías desproporcionadas al riesgo asumido o le impongan indebidamente la carga de la prueba en los casos en que debería corresponder a la otra parte contratante.

- Resulten desproporcionadas en relación con el perfeccionamiento y ejecución del contrato, como la imposición al consumidor de los gastos de documentación y tramitación que por ley corresponda al empresario.

- Contravengan las reglas sobre competencia y derecho aplicable como la previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor y usuario, al lugar del cumplimiento de la obligación o

aquél en que se encuentre el bien si éste fuera inmueble.

El listado completo está recogido en los artículos 85 a 90 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre.

Las prácticas de comercio electrónico abusivas más habituales son:

1) **Cartas nigerianas**: consisten en una inesperada comunicación mediante cartas y sobre todo a través de e-mails en las que el remitente promete negocios muy rentables. Se llaman cartas "nigerianas" porque en un principio, los remitentes se hacían pasar por ciudadanos de Nigeria o de otros países africanos. La expectativa de poder ganar mucho dinero mediante unas sencillas gestiones, es el gancho utilizado por los estafadores para que las potenciales víctimas olviden las más elementales precauciones.

¿Cómo funciona?

Un remitente desconocido contacta con la potencial víctima haciéndose pasar por un abogado, familiar o amigo cercano de un miembro del Gobierno o de un importante hombre de negocios que ha perdido la vida en un accidente o durante una revuelta política. Antes de morir esa persona, depositó una gran cantidad de dinero en una cuenta bancaria. El remitente asegura que tiene acceso legal a esa cuenta y pretende transferir el dinero a una cuenta en el extranjero. Ha encontrado el nombre y la dirección de la potencial víctima por recomendación de otra persona o por casualidad y la víctima es la única persona de confianza que puede ayudarle a realizar la transferencia del dinero.

Por su asistencia promete a la víctima un porcentaje de la cantidad total de dinero y solicita discreción para llevar a cabo el negocio. La víctima debe abrir una cuenta en un banco determinado para que pueda remitirle el dinero.

La siguiente fase del fraude consiste en convencer a la víctima de que la transferencia de dinero está en proceso. Para ello, mandan a la víctima documentos aparentemente oficiales, al igual que cartas y movimientos bancarios falsos. Se lleva a cabo un gran intercambio de cartas, e-mails, faxes y llamadas de teléfono entre los estafadores y su víctima para ganar su confianza y conseguir toda la información personal que sea posible.

Una vez que los estafadores han conseguido que la víctima confíe en ellos y convecerle de que está a punto de recibir todo el dinero, le comunican que han surgido unos problemas inesperados que impiden la entrega del dinero: es absolutamente imprescindible que la víctima pague unos impuestos, unas tasas especiales o unos honorarios a un abogado. Los estafadores aseguran que ese pago será el último que la víctima tenga que hacer.

Sin embargo, después de éste pago van surgiendo nuevos impuestos y tasas que pagar hasta que la víctima empieza a sospechar. Cuando la víctima deja de pagar, los estafadores desaparecen. En ocasiones, pasado un tiempo, vuelven a contactar con la víctima haciéndose pasar por investigadores que tienen conocimiento de la estafa y ofrecen su ayuda para recuperar el dinero. Este contacto tiene por objeto conseguir más dinero de la víctima con la excusa de cubrir los costes de las investigaciones.

¿Qué hacer si recibe una de estas cartas?

- No conteste.
- Nunca facilite sus datos bancarios ni personales.

¿Qué hacer si ya ha contactado con ellos o pagado alguna cantidad?

- Guarde todos los documentos que ha recibido y los mensajes que ha mandado.
- Guarde toda la documentación de las transacciones.
- Contacte con la policía y siga sus indicaciones.

2) **Phising**

¿Cómo funciona?

Los estafadores envían mensajes, haciéndose pasar por entidades bancarias que necesitan verificar datos, para conseguir información personal (números de la tarjeta de crédito, contraseñas, etc) de sus víctimas. En el mensaje que recibe la víctima se le pide que actualice o confirme información de su cuenta bancaria. Para ello, se pide que la víctima entre en un sitio web de apariencia similar a la de su banco real, pero no lo es. Se trata de un sitio creado por los estafadores con la única intención de engañar a la víctima e inducirla a que les suministre información para poder acceder a su cuenta bancaria.

¿Cómo evitarlo?

- Si recibe un e-mail en el que le solicitan datos personales o financieros no responda ni pinche en el link que aparece en el mensaje.
- Nunca facilite datos financieros a través de internet porque los bancos reales nunca los solicitan.
- Informe al banco del que supuestamente procede el e-mail.
- Utilice anti-virus y un Fire-wall y manténgalo actualizado. Algunos e-mails contienen software que puede dañar su ordenador o rastrear sus actividades en internet sin que usted se dé cuenta.

3) **Loterias**

La Lotería Nacional del Estado advierte sobre esta estafa en su página web. Las estafas de Lotería se están incrementando de manera alarmante.

En muchos casos los estafadores utilizan nombres como El Gordo, El Niño, etc., que inducen a creer que se trata de la Lotería Nacional del Estado.

¿Cómo funciona?

El funcionamiento es el siguiente: la víctima recibe un e-mail en el que se le informa de que ha ganado la lotería, a pesar de que no ha participado en ninguna clase de sorteo. Le piden que contacte con un agente para poder recoger el dinero. El consumidor contacta con el agente y éste le manda un formulario para verificar su identidad que debe rellenar y reenviar junto con copias de su pasaporte o DNI.

Una vez que el consumidor ha facilitado todos los datos recibe un e-mail en el que le ofrecen **tres posibilidades de cobro**: una transferencia bancaria, abrir una cuenta en un banco determinado para que ingresen el premio, o recoger el dinero personalmente (normalmente en país muy alejado del domicilio del consumidor). La mayoría de la gente opta por una transferencia bancaria a su cuenta y esto siempre supone la necesidad de pagos anticipados por honorarios de abogados, tasas, seguros, impuestos, etc. En estos casos se exige que los pagos se hagan a través de Western Union o compañías similares. En caso de que la víctima opte por abrir una cuenta en el banco que le indican los estafadores, se encontrará con que la política de ése banco exige que hagan un depósito de una cantidad importante de dinero para abrir la cuenta. Una vez efectuada la transferencia o realizado el depósito en la cuenta los estafadores desaparecen.

¿Qué hacer si recibe un mail comunicándole que ha ganado un premio?

- Si parece demasiado bueno para ser verdad, es probable que sea una estafa.

Recomendaciones:

- No responda a ninguno de estos mensajes.
- No envíe dinero.
- No envíe ni entregue documentos de identidad (ni siquiera copias).
- Nunca facilite datos de sus cuentas bancarias o tarjetas de pago.

¿Qué hacer si ha contactado con ellos o pagado alguna cantidad?

- Guarde todos los mensajes electrónicos y de texto que haya recibido o enviado.
- Guarde todos los documentos acreditativos de las transacciones o los pagos realizados.
- Denuncie inmediatamente a la policía de su localidad y siga sus indicaciones.
- Identificar un fraude no siempre es fácil. Sin embargo, la mayoría de los casos siguen un mismo patrón: se solicita al consumidor una cantidad de dinero por adelantado a cambio de recibir en un futuro una gran suma de dinero o productos a precios muy ventajosos o irrisorios.

Para ayudarle a reconocer un posible fraude, siga nuestras recomendaciones:

- Identifique al vendedor. Contraste al máximo la identidad e historial del vendedor. Para ello, puede consultar foros y opiniones.
- Si no encuentra datos de contacto o son dudosos, piénselo dos veces antes de pagar.
- Utilice medios de pago seguros. Los bancos y las entidades de pago por intermediación en Internet ofrecen herramientas que minimizan el riesgo.
- Nunca pague a través de empresas de envío de remesas de dinero. Si es posible, utilice una tarjeta de crédito ya que tendrá la posibilidad de devolver un cobro indebido.
- Busque sellos de confianza y conexiones seguras de Internet. Envíe información solo a través de páginas web con conexión segura, es decir, aquellas que empiezan por https.
- Use el sentido común.
- Desconfíe de ofertas demasiado buenas para ser verdad. Usar la lógica evita, en muchos casos, algunos contratiempos.

Documentos relacionados

Folleto, Falsificaciones: Fraudes y estafas comerciales

PARA SABER MÁS...

- Resolución Alternativa de Litigios (RAL)
- Impactos ambientales y alternativas al comercio online
- Compra segura en INTERNET GUÍA PRÁCTICA
- Fraudes y estafas comerciales
- El comercio electrónico superó en España los 12.400 millones de euros en el primer trimestre de 2021, casi un 2% más que el año anterior
- COMPRAR POR INTERNET: FÁCIL, RÁPIDO Y SEGURO
- Ver fichas Internet, dispositivos y pantallas, correo electrónico, publicidad, publicidad y marcas, gasto energético en el hogar, ocio y tiempo libre, consumo sostenible.