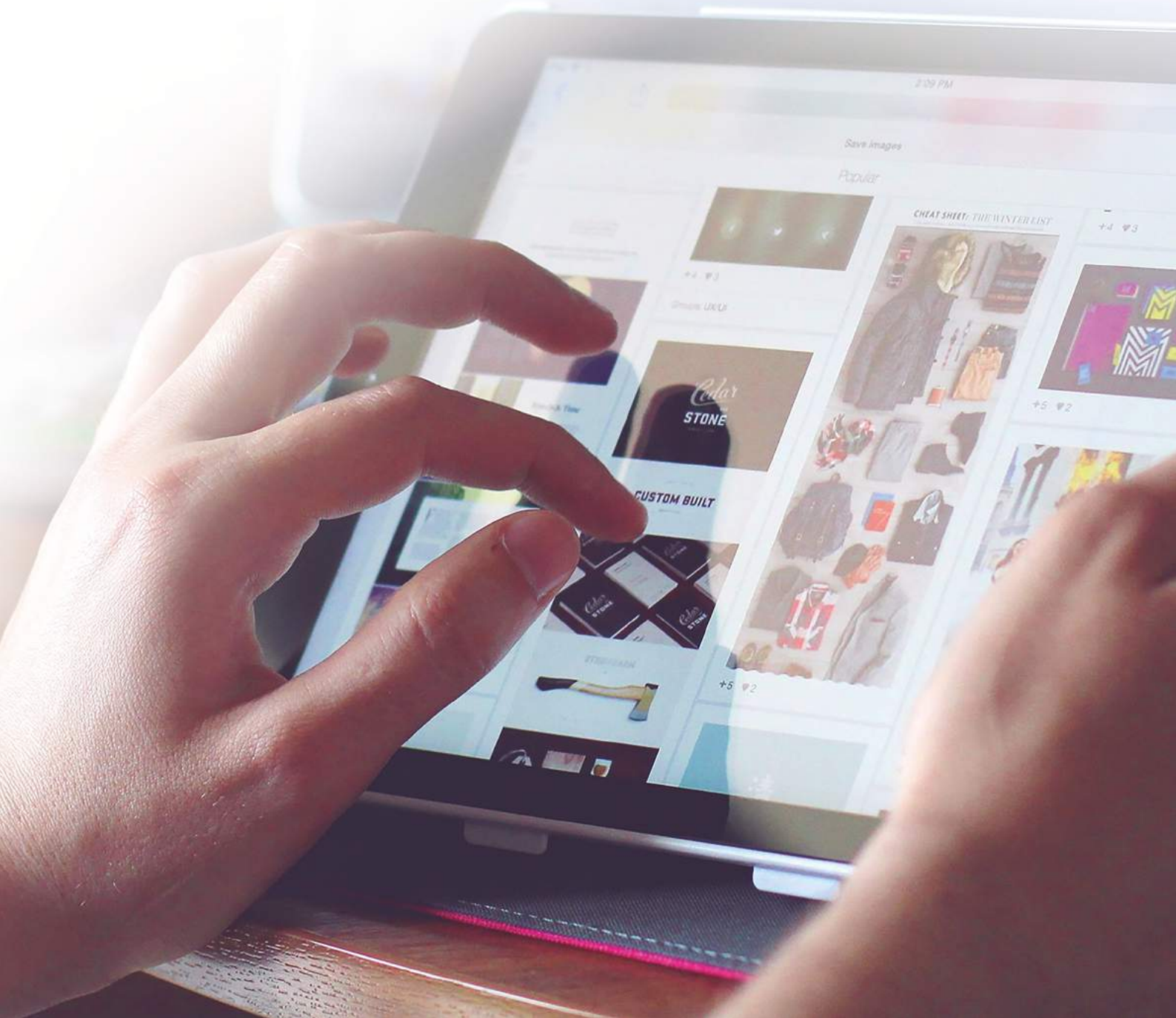
Compra segura en INTERNET

GUÍA PRÁCTICA



Compra segura en INTERNET

GUÍA PRÁCTICA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD

aecosan agencia española de consumo, seguridad alimentaria y nutrición

Policía Nacional

ÍNDICE

PRESENTACIÓN

El comercio electrónico constituye uno de los servicios de la sociedad de la información que ha experimentado un mayor crecimiento en los últimos años y representa una de las actividades con mayor potencial de futuro para la economía digital. En España, su facturación alcanzó los 24.185 millones de euros en 2016 y superó los 6.700 millones de euros en el primer trimestre de 2017, casi un 25% más que el año anterior, según datos de la Comisión Nacional de los Mercados y la Competencia (CNMC). De hecho, el porcentaje de usuarios que hacen pedidos de bienes y servicios online es del 50%, cuatro puntos por encima de la media de la UE, según Eurostat.

Por número de transacciones, el 44% de las compraventas realizadas se registran en webs españolas según la CNMC. El 93% de las compras que se realizan desde España hacia el exterior se dirigen a la UE.

Estas cifras ilustran la dimensión que ha adquirido el comercio electrónico en pocos años y la previsión de crecimiento futuro. Pero, junto a esta perspectiva económica, las instituciones públicas debemos velar por los derechos de los consumidores y usuarios que acceden a estos servicios a fin de poder ofrecerles la mayor protección posible antes, durante y después de la compra o contratación online.

A lo largo de cada una de estas fases, el consumidor y usuario de estos servicios puede encontrarse con un complejo y variado número de situaciones que requieran la actuación de aquellas instituciones públicas que proyectan sus competencias sobre esta actividad, cada una en sus respectivos ámbitos.

Esta Guía recoge de manera integral los derechos que asisten a los usuarios en los procesos de compra o contratación online, y ofrece consejos y recomendaciones desde diversos enfoques: la privacidad (Agencia Española de Protección de Datos), la seguridad (INCIBE), el consumo (AECOSAN) y la persecución de las prácticas delictivas o fraudulentas (Policía Nacional). La Guía está acompañada de siete fichas en las que se recogen de manera más concisa las principales cuestiones que debe tener en cuenta un usuario.

Además, promover prácticas que favorezcan el respeto a la protección de los datos personales, los derechos como consumidores, la seguridad de las redes y dispositivos con los que se realizan las transacciones comerciales y la persecución de las conductas fraudulentas son presupuestos indispensables para fomentar un clima de confianza y posibilitar la innovación y el crecimiento sostenible.

Esta Guía resultará de utilidad no sólo a los ciudadanos, como consumidores y usuarios de los servicios de comercio electrónico, sino también a las empresas que desarrollan su actividad en este ámbito. Para estas, la promoción de estas prácticas puede implicar una ventaja competitiva que debe potenciarse, ya que un ciudadano bien informado es clave para el crecimiento de cualquier negocio, y especialmente de aquellos que tienen lugar en el entorno digital, donde la confianza es la base del desarrollo de los nuevos negocios.

1.1. PUESTA A PUNTO DE LOS DISPOSITIVOS

1.1.1. Recomendaciones de seguridad básicas

Para realizar compras online con seguridad es fundamental que el dispositivo que se use esté debidamente configurado y protegido con el fin de evitar que una mala configuración de éste o una posible infección por malware permita que los datos intercambiados entre el usuario y la tienda online se vean comprometidos.

Medidas de protección preventivas:

- Instalar una herramienta antivirus y analizar el dispositivo antes de realizar la transacción para detectar posibles amenazas. Si el dispositivo está infectado, podría poner en riesgo la propia compra, así como la información asociada a ésta.
- Confirmar que el sistema operativo del dispositivo esté actualizado con la última versión, así como todos los programas y aplicaciones instaladas, para evitar que un fallo de seguridad en éstos permita a un ciberdelincuente tomar su control y ejecutar acciones maliciosas sin el conocimiento del usuario.
- Revisar los programas y las apps instaladas y eliminar todas aquellas que no se estén utilizando. Cuantas más tengamos, más difícil será mantener nuestro equipo actualizado y protegido, además de ralentizar y entorpecer su rendimiento.
- Evitar el uso de ordenadores, tabletas y teléfonos inteligentes públicos o compartidos para realizar compras online. Generalmente no podemos conocer su estado de seguridad o la finalidad de su uso (las páginas por las que se ha navegado), y podrían contener virus o cualquier otro tipo de código malicioso.

Más información en:

Links

- *Síntomas de los dispositivos infectados*
- *Herramientas antivirus gratuitas*
- *La importancia de las actualizaciones*
- *Cómo proteger los dispositivos y la información que contienen*
- *Consecuencias de no instalar las actualizaciones*
- *Consideraciones a tener en cuenta al utilizar ordenadores públicos*
- *Cómo actuar en caso de hacer uso de un dispositivo público*

1.1.2. Configuración de la red

Para realizar compras online en un entorno seguro, tan importante es configurar correctamente el dispositivo como utilizar una conexión de confianza que salvaguarde nuestra información.

Precauciones a tener en cuenta en redes WiFi

- No conectar el dispositivo a una red WiFi pública para realizar transacciones en las que hay intercambio de información confidencial, como es el caso de las compras online, el acceso a datos bancarios o pasarelas de pago, ya que el riesgo de que las comunicaciones sean interceptadas durante el proceso de compra es alto.

— Configurar el router WiFi doméstico adecuadamente para que terceros no puedan conectarse a la red.

Más información en:

Links

- *Protege tus dispositivos*
- *Riesgos de usar redes WiFi públicas*
- *Cuándo utilizar redes WiFi públicas*
- *Medidas básicas de configuración de redes WiFi*
- *Cómo asegurar la red WiFi en 7 pasos*
- *Te refrescamos cómo proteger la red WiFi de casa*

1.2. IDENTIFICACIÓN DE TIENDAS ONLINE DE CONFIANZA

1.2.1. Comprobar información legal del comercio

— La información de la tienda online, requerida por distintas normas legales, suele incluirse en páginas con denominaciones como "Aviso legal", "Términos de uso" o "Política de privacidad". Éstas suelen ser accesibles mediante enlaces ubicados en los extremos superior o inferior de la página principal del comercio online.

— La información legal es fundamental porque:

- Ante un posible conflicto permite saber contra quién debemos reclamar.
- Determina las leyes aplicables y las autoridades de control competentes.
- Permite conocer los derechos que asisten a los usuarios.

— Es obligatorio que el comercio online proporcione, entre otros, estos datos:

- Nombre completo de la entidad (persona física, sociedad, fundación, etc.)
- Número de identificación fiscal (NIF, NIE o CIF)
- Datos de su inscripción en el registro mercantil
- Dirección postal
- Dirección de correo electrónico

A partir del 25 de mayo de 2018, deberán añadirse, entre otros datos:

- El plazo de conservación de los datos
- La identificación del Delegado de Protección de Datos, si lo hay (el DPD es la persona que sirve de punto de contacto del comerciante para cualquier cuestión relativa al tratamiento de datos personales)

Más información en:

Links
- *Guía de Seguridad y Privacidad en internet*
- *Artículo 5 de la Ley Orgánica de Protección de Datos*
- *Artículo 13 del Reglamento General de Protección de Datos*
- *Artículo 10 de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico*

1.2.2. Identificar al titular/responsable del comercio

No se recomienda utilizar los servicios de un comercio online que no identifique debidamente a su responsable.

Una tienda online necesita recoger y tratar datos personales, tanto de sus clientes como de algunos usuarios aunque no sean clientes, por ejemplo, cuando se contacta para solicitar un presupuesto.

Los datos personales sólo pueden ser utilizados para aquellos fines de los que se ha informado a sus visitantes y clientes, y si alguno de ellos no guarda relación directa con la gestión de la compra, contratación o consulta (el caso típico es el envío de publicidad), deberá ofrecerse al usuario la posibilidad de oponerse a ese tratamiento en el momento de la recogida de datos.

En el caso de que los datos personales vayan a ser comunicados a otra entidad, es necesario que se informe previamente sobre la finalidad para la que se comunican, la identidad del destinatario y sus datos de contacto.

Quien proporciona datos personales a un comercio online no por ello deja de ser el titular de los mismos y, por tanto, le asisten los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). El comercio online debe informar de la posibilidad de ejercitar esos derechos y del procedimiento a seguir para hacerlo.

Más información sobre Derechos en el apartado 4 de esta Guía.

Links
- *Derechos ARCO y nuevos derechos del Reglamento*
- *Modelos para ejercer los derechos ARCO*

Ejemplo de texto legal correcto

Un comercio electrónico accesible en la dirección *www.micomercioelec.com* podría informar mediante un texto como el siguiente:

> *"La empresa titular de www.micomercioelec.com es MICOMERCIOE S.L, con domicilio en calle de la prueba, 1 2º B 28001 Madrid, con número de C.I.F: B-12345678, inscrita en el Registro Mercantil de Madrid en el tomo XX.XXX, folio XXX, sección X, hoja M-XXXXX (en adelante, MICOMERCIOE).*
>
> *MICOMERCIOE es el responsable del fichero en el que se incluirán los datos de los visitantes y usuarios de este sitio web. Sus datos son recogidos con las siguientes finalidades: la gestión de la relación comercial, el envío de comunicaciones publicitarias por distintos medios, incluidos los electrónicos.*
>
> ☐ *Me opongo a que mis datos sean tratados con finalidades publicitarias.*
>
> *Los visitantes y usuarios pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición ante MICOMERCIOE S.L., mediante escrito dirigido al domicilio postal arriba indicado o por correo electrónico a lopd@micomercioelec.com Las solicitudes deberán de ir acompañadas de una copia del documento acreditativo de la identidad del solicitante."*

Ejemplo de texto legal sin suficiente información

> *"El sitio web www.micomercioelec.com y todos sus contenidos son propiedad de micomercioelec. com.micomercioelec.com tratará los datos proporcionados en este sitio web respetando la LOPD. Si quiere contactar con nosotros en relación con sus datos personales puede hacerlo escribiendo a lopd@micomercioelec.com"*

Menores de edad

Los menores de 14 años no pueden prestar su consentimiento para que un comercio online recoja y trate sus datos personales; son sus representantes legales (padres o tutores) quienes pueden hacerlo en su nombre.

Aquellos comercios online que necesiten tratar datos de menores de 14 años deberán disponer de los medios para obtener el consentimiento de sus padres o tutores, por ejemplo, mediante un mensaje de correo electrónico dirigido a alguno de ellos que contenga un enlace a un formulario electrónico.

No se puede pedir a los menores de 14 años datos sobre el ámbito familiar. La única excepción son los datos de identificación y contacto de los padres o tutores, que podrán pedirse para poder solicitar a estos su consentimiento.

El Proyecto de Ley Orgánica de Protección de Datos, en tramitación parlamentaria en el momento en el que se publica esta Guía (diciembre de 2017), establece en 13 años la edad para que los menores puedan prestar su consentimiento.

Más información en:

Links · *Tú decides en internet*

Cookies

Al acceder a un comercio electrónico es posible que se descarguen en el equipo utilizado (ordenador, tablet, smartphone, etc) diferentes ficheros que recogen y almacenan información sobre nuestra navegación, conocidos como cookies.

El responsable de la página está obligado a informar sobre su uso y permitir al visitante o cliente elegir si los acepta o no.

La información sobre cookies ha de presentarse como un mensaje sobreimpreso en la parte superior o inferior de la página que proporciona la información básica (si se usan cookies, quién las usa y para qué las usa) y un enlace a otra página (política de cookies) dónde se dan más detalles sobre su uso y la manera en la que podemos rechazar parte o algunas de ellas.

El medio más sencillo para controlar el uso de cookies es la configuración del navegador, mediante la cual podemos:

- Rechazar todas las cookies
- Rechazar o aceptar cookies de determinados dominios
- Aceptar únicamente cookies de los sitios visitados y no de otros
- Hacer que todas las cookies se borren cuando cerramos el navegador

Más información en:

Links
- *Guía de Privacidad y Seguridad en internet*
- *Protege tu privacidad*
- *Guía sobre el uso de las cookies*

1.2.3. Verificar el titular y otros datos del registro del dominio

El dominio es la parte final de la dirección de internet que usamos para acceder a un sitio web o un comercio online. Por ejemplo, en www.agpd.es el dominio sería agpd.es.

Los dominios pueden ser registrados a nombre de una persona o de una organización (el registrante) a través de los servicios de un intermediario (el agente registrador).

Si tenemos dudas sobre un comercio online y la información legal que proporciona, es posible consultar quién ha registrado el dominio asociado al sitio web y comprobar si es quien se identifica como responsable del sitio web o alguien relacionado con él.

Más información sobre servicios de consulta de titularidad de dominios:

Links
- *Identifica sitios web en los que no debes confiar*
- *Consulta de dominios terminados en .es*
- *Consulta de dominios terminados en .eu*
- *Consulta del resto de dominios*

1.2.4. Comprobar que se trata de comunicaciones seguras (HTTPS)

Siempre que se proporcione información privada a través de internet (nombre, DNI, tarjeta de crédito, etc.), hay que comprobar que la página web o aplicación móvil envía la información utilizando el protocolo de comunicación seguro https. Este protocolo se utiliza para proteger la seguridad de la información intercambiada durante el proceso de compra. Se trata de garantizar que la información viaja cifrada para que nadie la intercepte, y que dispone de un certificado de seguridad válido que verifica la identidad del sitio web.

Las autoridades certificadoras son organismos independientes encargados de emitir certificados digitales. Actúan de mediador, y garantizan la legitimidad de un certificado digital mediante controles de seguridad y verificaciones para la emisión de cualquier certificado.

Consideraciones a tener en cuenta

- Comprobar que la web de la tienda online disponga de un certificado de seguridad. Si lo tiene, el navegador mostrará un icono con forma de candado y la URL empezará por https en lugar de http.
- Revisar que el certificado digital de la web es válido y corresponde con el sitio en el que realmente se quiere hacer la compra. Esta información se comprueba de forma distinta para cada navegador, aunque por lo general será haciendo clic sobre el icono con forma de candado. Se debe verificar quién ha emitido el certificado (autoridad certificadora), para quién (nombre de la empresa de la tienda online y dominio) y su plazo de validez.
- Si una tienda online no dispone de certificado, o éste no es válido, se recomienda no continuar con el proceso de compra y buscar otra web que cumpla con los requisitos mínimos de seguridad recomendados.
- En el caso de las aplicaciones móviles, éstas deben informar sobre los mecanismos de seguridad que utilizan para proteger la información y datos personales en los procesos de compra, pero recomendamos seguir las indicaciones contempladas en el apartado 1.3.6 de esta Guía.

Más información en:

Links
- *Información sobre el candado que aparece en los navegadores*
- *Cómo comprobar certificados digitales*

1.2.5. Sellos de confianza

Los sellos de confianza son distintivos que se proporcionan a las tiendas online para demostrar su calidad y seguridad en la venta online. Para conseguir el sello, éstas son auditadas o evaluadas para comprobar que cumplen criterios de seguridad en la compra y cumplimiento legal en materia de privacidad y protección de los consumidores.

Las tiendas que tienen un sello de confianza están adheridas a un código de conducta y suelen ofrecer a los consumidores procedimientos alternativos de resolución de conflictos sencillos, rápidos y cómodos.

Siempre que se desee llevar a cabo una compra hay que comprobar si la tienda online está adherida a un código de buenas prácticas de comercio electrónico.

Si el comercio online dispone de un sello, lo más probable es que lo muestre en su página principal y que contenga un enlace a la página web de la organización que concede los sellos. En esa página podrá encontrar las ventajas que concede a sus usuarios concretamente ese sello de confianza.

Uno de los sellos de confianza más conocido en España es *Confianza Online*.

Más información en:

Links
- *Sellos de confianza*

1.3. DETECCIÓN DE FRAUDES

1.3.1. Phishing

El phishing es uno de los métodos más utilizados para obtener información de los usuarios de forma fraudulenta a través de internet suplantando la identidad de páginas de servicios conocidos, instituciones públicas, redes sociales, así como de bancos, cajas y otras entidades financieras.

Consiste en hacerse pasar por un servicio web conocido para el usuario para engañarle y solicitarle contraseñas, datos personales o bancarios, que luego utilizará o venderá a terceros para cometer otros fraudes. Para obtener esta información, los ciberdelincuentes generalmente facilitan un enlace que redirige al usuario a una página web fraudulenta que simula ser la legítima.

Consejos para evitar ser víctima de phishing

- Hay que sospechar de mensajes alarmistas o que llamen la atención del usuario y que suelen tener como finalidad que éste acceda a un enlace o descargue un fichero adjunto de manera inminente.
- No se debe responder a correos electrónicos o mensajes que se reciben sin esperarlos y que solicitan datos personales o bancarios. Hay que contrastar la información preguntando directamente a las partes implicadas en el mensaje o acudiendo a terceros de confianza: Fuerzas y Cuerpos de Seguridad del Estado, INCIBE, AEPD, etc.
- Del mismo modo, si se recibe un mensaje de un usuario desconocido o aun siendo conocido, el contenido es sospechoso, hay que ser cautos y no hacer clic en los enlaces que pueda contener.
- Ninguna entidad, empresa o servicio con buena reputación solicitará datos de acceso a sus cuentas online u otros datos relacionados con el usuario bajo ninguna excusa a través del correo electrónico. Si se recibe un mensaje en este sentido, hay que eliminarlo. En caso de duda, siempre se puede preguntar a través de los canales oficiales directamente a la empresa o servicio mencionado.

Más información en:

Links
- *En qué consiste el phishing*
- *Cómo identificar un phishing*
- *Phishing; el fraude que intenta robar nuestros datos personales y bancarios*

1.3.2. Carding

Actividad delictiva consistente en la utilización fraudulenta de numeraciones válidas de tarjetas de crédito/debito para efectuar compras por internet en comercios virtuales.

Esta modalidad afecta principalmente a la tienda online. Si se llevan a cabo compras de manera fraudulenta, el titular de la tarjeta con la que se realiza el pago tendrá que efectuar la correspondiente denuncia y reclamar la devolución de los cargos efectuados.

Consejos y recomendaciones

- Realizar una revisión periódica de los movimientos de nuestras cuentas a las que tengamos asociadas tarjetas por si vemos algún cargo sospechoso y, en su caso, poder reclamar.
- Es imprescindible anular las tarjetas en caso de pérdida o sustracción.

1.3.3. Páginas de venta online falsas

Hoy en día es relativamente sencillo crear una página web falsa simulando ser un comercio online cuando en realidad es un fraude. El producto o servicio adquirido por el usuario nunca llegará a entregarse, dado que detrás de dicha página web no existe ningún soporte comercial.

Consejos para evitar compras en tiendas falsas

- Realizar preferentemente las compras en páginas oficiales o con reputación y prestigio consolidado.
- No se recomienda comprar si no aparece en la web información sobre:
  - Datos reales y físicos de la empresa: titular, NIF/CIF, domicilio fiscal, etc.
  - Condiciones de venta, devoluciones o reclamaciones
  - Textos legales: aviso legal, políticas de privacidad, etc.
- Sospechar de tiendas con precios muy por debajo del precio de mercado, o si todos los productos se venden al mismo precio, independientemente del modelo.
- En cuanto al diseño de la web, desconfiar:
  - Si no transmite homogeneidad (varios tipos de letra en la misma ventana)
  - La foto de portada puede encontrarse en otros lugares de internet
  - La calidad de las imágenes no es buena: pixeladas, de baja calidad o incluyen marcas de agua
  - La web aparenta ser la página legítima de una determinada marca
  - Aparecen textos mal traducidos. Por ejemplo, aparece traducida la sección “Home” como “Casa”, en lugar de “Inicio”, que es lo comúnmente utilizado
- Descartar la compra si la web anuncia varias formas de pago, pero finalmente sólo acepta tarjeta de crédito

Más información en:

Links

- *Evita fraudes en falsas tiendas online (I de II)*
- *Evita fraudes en falsas tiendas online (II de II)*
- *Yo no compraría en una tienda online si…*
- *¿Será fiable esta página?*

1.3.4. Estafas a través del correo electrónico

Modalidad de estafa consistente en aprovechar las actividades de compra por internet de comercios que distribuyen a terceros países, con los que el comprador mantiene una relación habitual a través de correo electrónico.

La actividad delictiva consiste en acceder por distintos mecanismos (malware, intrusión, etc.) al tráfico de mensajes entre el comercio y su distribuidor. Los estafadores, haciéndose pasar por los distribuidores legítimos del comercio, inducen a este último a realizar los pagos por la compra de la mercancía a cuentas bancarias o sistemas de dinero virtual controlados por ellos.

Consejos y recomendaciones

- Si existe una relación comercial previa, hay que desconfiar de movimientos, solicitudes o peticiones inusuales.

1.3.5. Delitos contra la propiedad industrial e intelectual

- Respecto a los productos de lujo o marcas de alta gama, desconfiar cuando su precio está muy por debajo del precio del mercado, ya que podría tratarse de productos falsificados o robados.
- Si el comprador adquiere productos a sabiendas de su falsedad, o de su ilícita procedencia, podría incurrir en un delito de receptación con resultados penales.
- Debe extremarse la prudencia respecto de los sitios que, tras un registro previo como, por ejemplo, solicitando una dirección de correo electrónico, una respuesta a un SMS o similar, ofrecen la posibilidad de descargarse o acceder en streaming a discos, películas, series, libros y otros productos similares de modo gratuito, ya que podría tratarse de productos obtenidos sin la autorización de los titulares de los derechos de autor.

Consejos y recomendaciones

- Se debe comprar siempre en páginas oficiales y/o de confianza, sin caer en provocaciones de “gangas imposibles”.
- Si existen razones fundadas que indiquen que el producto adquirido se trata de una falsificación, se denunciará en Dependencias Policiales.
- Es recomendable informar sobre este tipo de venta a las organizaciones o autoridades de consumo.

1.3.6. Aplicaciones fraudulentas o de dudosa reputación

Los dispositivos móviles son una herramienta muy potente que utilizamos para prácticamente todo: comunicarnos con otras personas, monitorizar la actividad física, obtener ubicaciones, consultar movimientos bancarios o realizar compras online mediante las aplicaciones disponibles para tal fin. De la misma forma que debemos verificar la seguridad de un sitio web tradicional, hemos de hacerlo con las aplicaciones que descargamos para realizar compras en internet.

Consejos para no instalar apps maliciosas

- Hay que asegurarse que se descarga la app oficial, es decir, que no se trata de una suplantación de la legítima. Comprobar cuál es la entidad que figura como desarrollador de la aplicación es una buena práctica, así como la política de privacidad.
- Revisar los permisos de la app para tener bajo control qué solicita al instalarse y para qué. Valorar si los permisos que solicita son razonables para el funcionamiento que ofrece.
- Consultar los comentarios y la valoración que han realizado los usuarios sobre la app antes de instalarla o comprar a través de ella. Las opiniones pueden ayudar a identificar si se trata de una app fraudulenta o de mala reputación.
- El número de descargas de la app también da pistas sobre la misma. Por ejemplo, si se trata de una app muy conocida y cuenta con pocas descargas, es probable que no se trate de la aplicación oficial y, por tanto, hay que ponerla en cuarentena y revisar el resto de indicaciones para valorar su fiabilidad.
- Evitar siempre descargar apps de repositorios no oficiales, ya que no hay ninguna garantía de seguridad de las aplicaciones allí alojadas y cualquiera ha podido manipularlas.
- Leer la política de privacidad, pago y seguridad.

Más información en:

Links
- *Apps para dispositivos móviles ¿nos podemos fiar de todas?*
- *Apps y robo de información*
- *Por qué evitar apps que requieren de muchos permisos para su uso*

1.3.7. Servicios de compraventa o de venta de segunda mano

En los últimos años han aparecido nuevos servicios online que facilitan la compra y venta de artículos y productos de segunda mano. Dichos servicios actúan como intermediarios entre el comprador y el vendedor, permitiendo la publicación de anuncios en los que el vendedor describe las características del producto, el precio de venta, así como los mecanismos de contacto. A pesar de que estos servicios ofrecen muchas ventajas, no están exentos de riesgos que se deben conocer para evitar fraudes en la compra o venta de un producto.

Algunos consejos

Si se quiere comprar:

- Obtener información sobre quién es el vendedor antes de realizar la compra: realizar búsquedas por el nombre, ver comentarios y valoraciones de otros usuarios, etc.
- Descartar anuncios que contienen fotos genéricas del artículo en venta, o cuya redacción no esté cuidada, parezcan traducciones automáticas y/o cuya descripción no coincida con el artículo en venta.
- Si el vendedor se encuentra en el extranjero y utiliza este hecho como excusa para que la gestión de los trámites se ejecute de una forma determinada, no continuar con la compra.
- No aceptar nunca como método de pago para este tipo de compras servicios como Western Union o Money Gram.
- Cancelar el proceso de compra en caso de dudas.

Si lo que se pretende es vender:

- Hay que informarse sobre quién es el comprador antes de realizar el envío.
- Sospechar si ofrecen más dinero del que se pide en el anuncio.
- Utilizar un método de pago conocido que garantice que la compra está bajo nuestro control y no en manos del comprador.
- No adelantar dinero. En algunas estafas, el comprador utiliza como excusa que su banco no le permite realizar transferencias inferiores a una cantidad de dinero que, casualmente, es siempre mayor que el precio del artículo en venta. El objetivo es intentar engañar al vendedor para que abone por adelantado la diferencia de dinero para compensar los costes totales a través de servicios como Western Union.
- Cancelar el proceso de venta en caso de dudas.

Más información en:

Links

- *Servicios compraventa y subastas*

2.1. MEDIOS DE PAGO PARA COMPRAS ONLINE

Una de las mayores preocupaciones de los usuarios al realizar compras online es el tipo de pago a utilizar. Aún son muchos los que desconocen las distintas alternativas disponibles y qué ventajas o inconvenientes aporta cada una. Por tanto, es importante conocer qué opciones hay disponibles para saber cuál es la que más interesa utilizar para cada tipo de compra y la que ofrece una mayor seguridad.

A continuación se describen los medios de pago de uso común en el comercio online y, para cada uno de ellos, los derechos que asisten a los consumidores y los aspectos más relevantes en cuanto a la seguridad que ofrecen.

2.1.1. Envíos de dinero en efectivo

- Determinados servicios están diseñados para realizar transferencias de dinero, incluso de forma anónima, resultando imposible identificar quién es el emisor y el receptor y, por tanto, no se deben utilizar nunca para realizar compras online.

- **Derechos.** Uno de los aspectos principales del comercio electrónico, junto con la seguridad, son los medios de pago utilizados. Si un operador de comercio online solicita el pago en dinero efectivo, renuncia a la compra o a la contratación.

- **Seguridad.** Aunque este sistema no supone un intercambio de datos bancarios entre vendedor y comprador, no es un método seguro para realizar compras online ya que no hay constancia de quién envía el dinero ni tampoco de quién lo recibe, por lo que se pierde la trazabilidad del mismo. Por tanto, en caso de problemas con la compra (producto que no llega, defectuoso o incorrecto) será difícil reclamar el dinero, ya que no se sabe a ciencia exacta quién retiró el cheque con el dinero, especialmente en caso de ser víctimas de un fraude.

2.1.2. Contra reembolso

- Es la modalidad de envío de paquetes, en la cual se paga en efectivo cuando se recibe el paquete.

- **Derechos.** Para el comprador se trata de un sistema bastante fiable, ya que se paga el producto cuando se recibe. Sin embargo, en muchas tiendas online no se ofrece esta posibilidad por el riesgo que supone asumir el envío de un producto que aún no ha sido pagado y, además, le puede generar un coste adicional de gastos de envío si en el momento de la entrega no se encuentra el cliente en el domicilio. Por otro lado, puede resultar poco práctico para el cliente, especialmente cuando los costes del efectivo a pagar son elevados.

- **Seguridad.** Es un método muy seguro, ya que sólo se paga el producto cuando se recibe y después de abrir el paquete y comprobar que el pedido es correcto.

2.1.3. Transferencia bancaria

- Este método de pago permite enviar una cantidad de dinero desde una cuenta bancaria a otra. La principal ventaja respecto a otros medios de pago es que no es necesario introducir ningún dato en el sitio web. Sin embargo, no todas las tiendas virtuales ofrecen esta opción de pago.

- **Derechos.** En el caso de no entregar los bienes o servicios adquiridos se puede reclamar contra el proveedor, por incumplir el objeto del contrato.

- **Seguridad.** El vendedor sólo tendrá que facilitar los datos de la cuenta bancaria para que el comprador proceda a realizar el ingreso del dinero correspondiente a su compra. Sin embargo, puede suponer riesgos de seguridad, especialmente en caso de transferencias internacionales ya que el dinero será difícil de recuperar una vez abonada en la cuenta del receptor. Si el titular de la cuenta receptora del dinero no autoriza su devolución, habría que acudir a la vía judicial.

2.1.4. Pago con tarjeta

- Es la modalidad más utilizada por las tiendas virtuales. La única información necesaria para realizar el pago está contenida en la propia tarjeta de crédito/débito.

- **Derechos.** Los beneficiarios de las operaciones de pago no podrán exigir al consumidor el pago de gastos o cuotas adicionales por la utilización de la tarjeta.

  Cuando el importe de una compra ha sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, el consumidor y usuario titular de ella podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del vendedor y del cliente titular de la tarjeta se efectuarán a la mayor brevedad.

  Si la compra ha sido efectivamente realizada por el titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento, el comprador quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación.

  En el caso de servicios continuados que se abonan periódicamente, hay que advertir de que el pago con tarjeta es un sistema menos garantista para el consumidor que la domiciliación, ya que en ésta basta con devolver los recibos incluso a posteriori, mientras que la recuperación de importes abonados por tarjeta es más compleja.

- **Seguridad.** Aunque implique el intercambio online de datos bancarios, puede llegar a ser un sistema de pago muy seguro siempre que la tienda online utilice una pasarela de pago que ofrezca algún banco, el cual se encargará de verificar la autenticidad de la tarjeta y de la protección de los datos del cliente. De este modo, la tienda online en ningún momento dispondrá de los datos financieros del usuario, lo que dota de mayor seguridad al proceso de pago. En el caso de que la tienda no utilice la pasarela de pago seguro del banco, la protección de los datos bancarios del comprador recaerá sobre la propia tienda y los mecanismos de seguridad que tenga implantados. Por tanto, si hay dudas sobre la fiabilidad de la web, es mejor descartar la compra y no facilitar los datos de la tarjeta de crédito para que no se haga un uso indebido de los mismos.

  Asimismo, cuando sea posible, se recomienda valorar la posibilidad de disponer de una tarjeta de uso exclusivo para realizar pagos online; es posible que incluso podamos desactivar esta tarjeta cuando no la necesitemos si realizamos compras online de forma ocasional.

2.1.5. Pago a través de intermediarios

- Modalidad de pago en la que se utiliza a una tercera empresa de confianza, por ejemplo PayPal, para que gestione los datos bancarios tanto del vendedor como del comprador y se encargue de formalizar los pagos. De esta forma, no es necesario que el vendedor conozca los datos de comprador y viceversa. Muchas tiendas online ofrecen este servicio por su comodidad para el usuario al no tener que introducir sus datos bancarios cada vez que va a realizar una compra.

- **Derechos.** Antes de adherirse a este sistema de pago se recomienda a los consumidores y usuarios que consulten las condiciones de uso del servicio.

- **Seguridad.** Sistema de pago muy seguro siempre que el usuario utilice una contraseña robusta para acceder al servicio. El usuario solo necesita disponer de una cuenta y configurar en ella su tarjeta de crédito. Cuando se realice una compra online utilizando este sistema de pago, los datos financieros del cliente no los manejará el vendedor y viceversa, será la tercera empresa de confianza quien se encargue de realizar la gestión correspondiente con cada una de las partes, lo que dota de mayor seguridad al proceso.

Más información en:

Links

- *¿Cómo crear contraseñas seguras?*
- *¿Son suficientes las contraseñas?*
- *¿Qué tipo de pago online se adapta a mis necesidades?*
- *Seguridad en PayPal*
- *Información sobre Verified by Visa*
- *Información sobre MasterCard SecureCode*

2.2. CONFIGURACIÓN DE LAS CUENTAS DE USUARIO

2.2.1. Contraseñas seguras

Muchas tiendas online obligan a disponer de una cuenta de usuario a través de la cual configurar ciertos parámetros, como nombre y apellidos, dirección de envío del pedido, domicilio para registrar la factura, datos de la tarjeta de crédito, etc. Para proteger el acceso a esa información, el mecanismo facilitado es la contraseña. La fortaleza de esa contraseña determinará si los datos almacenados en la cuenta de usuario están más o menos protegidos del acceso de intrusos o personas no deseadas. Por este motivo, es de vital importancia utilizar contraseñas seguras y gestionarlas correctamente para que nadie las adivine o las obtenga probando distintas combinaciones de letras y números.

Cómo generar contraseñas seguras

- Debe tener una longitud mínima de ocho caracteres, combinando letras mayúsculas y minúsculas, números y caracteres especiales (símbolos).
- Nunca se deben utilizar como contraseñas palabras sencillas en cualquier idioma que se puedan encontrar fácilmente en el diccionario.
- Cuidado con informaciones muy obvias relacionadas con la persona: nombres propios, de mascotas, lugares significativos, fechas de nacimiento o de otros eventos especiales, etc.
- Evitar contraseñas formadas únicamente a partir de la concatenación de varios elementos. Por ejemplo: "Marco1978" (nombre + fecha de nacimiento).
- Y por supuesto, no usar ninguna de las siguientes contraseñas, ni similares: 123456, 123456789, qwerty, 12345678, 111111, 1234567890, 1234567, password, 123123, 987654321.

Más información en:

Links

- *¿Por qué son tan importantes las contraseñas?*
- *Cómo generar contraseñas seguras (vídeo)*
- *Por qué no utilizar la misma clave para distintos servicios (infografía)*
- *Cómo prevenir el robo de contraseñas*
- *Cómo utilizar un gestor de contraseñas (vídeo)*
- *Quiero proteger mi correo electrónico*

2.2.2. Activar verificación en dos pasos o doble verificación

En ocasiones, una contraseña robusta no garantiza totalmente la seguridad de la cuenta. Por ejemplo, si el equipo está infectado con algún virus, o el smartphone o tablet tienen instalada alguna app maliciosa diseñada para robar las contraseñas de acceso del usuario. Por otro lado, es posible que, en un momento dado, el usuario engañado bajo un falso pretexto acabe facilitando a los ciberdelincuentes sus datos de acceso a un determinado servicio (un ejemplo típico es el phishing).

Afortunadamente, para protegerse de estos riesgos, muchos servicios online y algunas tiendas virtuales ofrecen la opción de activar la doble verificación.

Qué es la doble verificación

- Consiste en solicitar al usuario un PIN, código o clave adicional durante el proceso de login/registro o durante el proceso de formalización de la compra.
- Dicho código sólo lo conocerá el usuario.
- Lo recibirá a través de un canal al que sólo él tiene acceso, por ejemplo, en su teléfono móvil.

Más información en:

Links

- *¿Son suficientes las contraseñas?*
- *Verificación en dos pasos, ¿qué es y cómo me puede ayudar?*
- *Añade una capa de seguridad extra a la cuenta de usuario*

2.2.3. Recuperación de cuentas

Puede ocurrir que el usuario olvide la contraseña de acceso a la cuenta personal de la tienda online donde quiere tramitar una compra. Los servicios online permiten recuperar el control de la cuenta al usuario mediante diversos mecanismos. Los más frecuentes son la recuperación de la contraseña haciendo uso del correo electrónico y de preguntas de seguridad.

Es importante tener en cuenta algunos aspectos de seguridad para que estos mecanismos de recuperación no sean utilizados por usuarios con malas intenciones, ya que si alguien consiguiese recuperar el control de una cuenta de una tienda online en la que hay datos financieros registrados, podría, por ejemplo, ejecutar compras sin que el dueño de la cuenta sea consciente de ello hasta que vea los cargos en su cuenta bancaria.

Aspectos a tener en cuenta para la recuperación de cuentas de usuario

— Al recuperar una contraseña a través del correo electrónico:

- Deberá asegurarse de que la contraseña de acceso al correo cumple con los requisitos mínimos de seguridad exigidos.
- La contraseña de acceso al correo debe ser diferente a la de la cuenta de la tienda online. Nunca deben utilizarse las mismas contraseñas para servicios diferentes.
- Si el servicio online lo permite en su configuración, utilizar un correo electrónico alternativo al empleado en el proceso de registro para la recuperación de la contraseña.

— Al recuperar una contraseña a través de pregunta secreta:

- Generalmente hay que configurar manualmente esta opción. Comprobar si la tienda online donde se va a comprar dispone de esta funcionalidad.
- Las respuestas no deben estar basadas en información verídica, ya que, aunque generalmente son más fáciles de recordar, si alguien conoce mínimamente a la persona, personalmente o por la información publicada en internet, podría ser relativamente sencillo adivinar las respuestas.
- Deben ser fáciles de recordar por el usuario y guardarse de un modo seguro. Hay que tener en cuenta que en la mayoría de los casos se utilizan muy esporádicamente, sólo en caso de pérdida de la contraseña principal, y es necesario recordar o recuperar fácilmente esos datos.

2.2.4. Cuándo guardar información de los métodos de pago

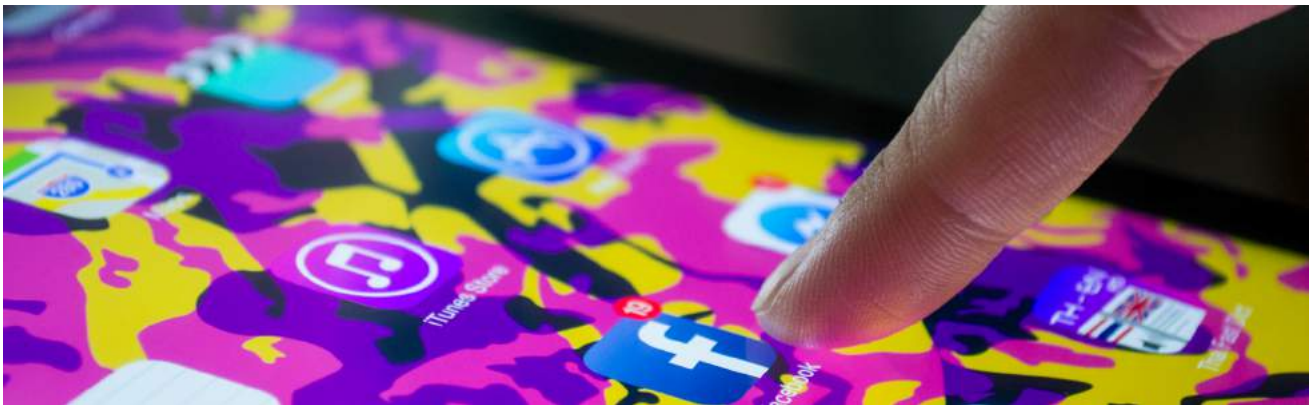
Después de realizar una compra online, posiblemente en la cuenta de usuario se han memorizado datos como nombre, dirección de envío y de facturación, histórico de compras, número de teléfono, etc. Pero también la información relativa a la forma de pago utilizada, que en la mayoría de los casos será la tarjeta de crédito: tipo de tarjeta, número, fecha de caducidad y CVV. Si es así, habrá que valorar si interesa que los datos financieros se almacenen en la cuenta para futuras compras o, por el contrario, es preferible borrarlos.

Consideraciones a tener en cuenta

Si la cuenta de usuario de la tienda online no está correctamente configurada en cuanto a seguridad (contraseña robusta, doble verificación), se desaconseja totalmente mantener almacenada información financiera. Especialmente si se trata de una tarjeta de crédito asociada a una cuenta corriente con dinero suficiente como para realizar distintos cargos.

Es preferible introducir estos datos en cada proceso de compra que asumir el riesgo de que alguien capture las contraseñas de acceso a la cuenta y proceda a realizar compras online a cargo del usuario víctima.

Y hay que recordar siempre que, independientemente de si se almacena esta información o no en la cuenta de usuario, al finalizar debe cerrarse siempre la sesión al terminar la compra para evitar que nadie acceda a ella.



2.2.5. Consideraciones específicas para compras a través de apps

En el caso de compras online a través de apps, es importante tener en cuenta además algunas cautelas adicionales para evitar que nadie realice compras en nombre de otra persona si, por algún motivo, tiene acceso físico al terminal móvil donde está configurada la app de compra online con los datos privados y bancarios previamente configurados.

Medidas de seguridad extra para compras a través de apps móviles

- Establecer un bloqueo de pantalla del dispositivo con el menor tiempo de espera posible para restringir el acceso a las funcionalidades incluyendo las apps. Es posible configurar un patrón, PIN o contraseña siendo las opciones más seguras las dos últimas.

- Proteger el acceso a aplicaciones concretas para que no las pueda iniciar cualquier persona. Es una opción muy interesante para aquellas apps, como muchas de compras online, que dan acceso a servicios que proporcionan información sobre el usuario y que, por defecto, guardan la sesión no siendo necesario introducir la clave de acceso cada vez que se quieren utilizar. Algunas aplicaciones traen incorporada esta medida de seguridad pero, para aquellas en las que no sea el caso, es posible instalar una "app locker", como así se conocen, que ofrezca esta funcionalidad.

- De manera adicional, se recomienda configurar el dispositivo para que antes de descargar cualquier aplicación del repositorio de aplicaciones, de pago o no, sea necesario introducir un código PIN que apruebe la acción. De esta forma, se evitará que personas sin permisos instalen o utilicen aplicaciones sin consentimiento del dueño del dispositivo.

3.1. DERECHO DE DESISTIMIENTO

Es la facultad del consumidor y usuario de dejar sin efecto el contrato celebrado, notificándoselo así a la otra parte contratante en el plazo establecido para el ejercicio de ese derecho, sin necesidad de justificar su decisión, sin penalización de ninguna clase y sin gasto alguno para el consumidor y usuario.

El consumidor y usuario dispondrá de un plazo de 14 días naturales para ejercer este derecho, que se computará desde la recepción del bien objeto del contrato o desde la celebración de éste si su objeto fuera la prestación de servicios. En caso de que no se informe al usuario de la existencia de este derecho, el plazo se amplía a doce meses.

Su ejercicio no implicará gasto alguno para el consumidor y usuario.

Cuando el consumidor y usuario haya ejercido el derecho de desistimiento, el comercio online estará obligado a devolver las sumas abonadas por éste sin retención de gastos y sin demoras indebidas, en cualquier caso, antes de transcurridos 14 días naturales desde la fecha en que haya sido informado de la decisión de desistimiento por el consumidor y usuario.

El comercio online deberá informar al consumidor por escrito en el documento contractual, de manera clara, comprensible y precisa, de este derecho y de los requisitos y consecuencias de su ejercicio, incluidas las modalidades de restitución del bien o servicio recibido. Deberá entregarle, además, un documento de desistimiento, identificado claramente como tal, que exprese el nombre y dirección de la persona a quien debe enviarse y los datos de identificación del contrato y de los contratantes a que se refiere.

Algunas excepciones al derecho de desistimiento

- Billetes de avión y tren, entradas de conciertos, reservas de hotel y de alquiler de vehículos y servicios de suministro de comidas para fechas específicas.
- Alimentos y bebidas servidas habitualmente a domicilio (reparto de supermercados, por ejemplo).
- Artículos fabricados a medida o personalizados (un traje hecho a medida, etc.) soportes de datos de audio, vídeo o software informático precintados (como DVD) que se hayan abierto.
- Contenidos digitales online, si ya se ha iniciado la descarga o la emisión en tiempo real.
- Productos comprados a particulares y no a empresas.
- Contratos de reparaciones y trabajos de mantenimiento urgentes una vez acordado el precio del servicio.

Más información en:

Links
- *Derechos del consumidor*
- *Resolución de Conflictos de Consumo*

3.2. GARANTÍAS

Los productos adquiridos a través de una tienda online se regirán por el régimen de garantías en la venta de bienes de consumo.

La garantía en la compra de un artículo nuevo es de dos años, sea cual sea el canal a través del cual se adquiera. Esta garantía de dos años es un derecho mínimo; es posible que las leyes nacionales ofrezcan una mayor protección.

Las garantías a las que tiene derecho el consumidor se aplicarán tanto a productos nuevos como de segunda mano, si bien estos últimos cuentan con alguna particularidad, como es el plazo máximo de un año en defecto de pacto entre comprador y vendedor. En todo caso, el consumidor tiene derecho a recibir un producto en perfecto estado.

La reparación y la sustitución serán gratuitas para el consumidor. Comprenderán los costes necesarios para subsanar la falta de conformidad de los bienes con el contrato, especialmente los gastos de envío así como los relacionados con la mano de obra y los materiales, y se llevarán a cabo en un plazo razonable. Mientras que el producto permanezca en el servicio técnico del vendedor (que puede ser el del fabricante) se suspende el cómputo del tiempo de la garantía.

3.3. PRODUCTO DEFECTUOSO: GASTO DE ENVÍO Y REENVÍO

Un producto defectuoso es aquel que no ofrece la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razonablemente previsible del mismo y el momento de su puesta en circulación.

Los oferentes serán responsables de los daños causados por los defectos de los productos que, respectivamente, fabriquen o importen.

Según la normativa de la Unión Europea, si el producto comprado es defectuoso o no responde a las características anunciadas u ofertadas, incluyendo precio, impuestos aplicados y gastos de entrega, el consumidor puede optar entre:

- La reparación del bien
- Su sustitución
- Una rebaja del precio
- La resolución del contrato con devolución del importe, salvo que una de ellas resulte imposible o desproporcionado. En principio, se entiende como desproporcionada aquella medida que imponga al vendedor costes que, en comparación con la otra posibilidad, no sean razonables

3.4. DERECHOS SOBRE LOS DATOS PERSONALES

Después de haber contactado, comprado o contratado en un comercio online, éste conservará los datos personales que se le hayan proporcionado y podrá tratarlos para aquellos fines para los que haya obtenido consentimiento.

Los derechos ARCO permiten ejercer el control sobre nuestros datos, aunque se encuentren en los sistemas informáticos del comercio online.

El ejercicio de los derechos debe hacerse por los propios visitantes o clientes o por sus representantes legales.

Los derechos que asisten a los menores de 14 años deberán ser ejercidos por alguno de sus representantes legales. En el Proyecto de Ley Orgánica de Protección de Datos se establece la edad en 13 años.

En caso de no obtener respuesta del comercio online ante la solicitud de ejercicio de esos derechos, o de que ésta no sea satisfactoria, el usuario puede interponer una reclamación ante la Agencia Española de Protección de Datos.

Derecho de acceso

- Permite al usuario conocer qué datos personales suyos tiene el comercio online y acceder a ellos.
- El comercio online deberá contestar a la solicitud en el plazo de un mes, a contar desde su recepción, bien proporcionando los datos solicitados o bien motivando su negativa (por ejemplo, porque no dispone de ellos).

Derecho de rectificación

- Permite corregir errores, modificar los datos que sean inexactos o incompletos y garantizar la certeza de la información de que dispone el comercio online. Un ejemplo sería para actualizar una dirección de facturación o un teléfono de contacto.
- El comercio online deberá contestar a la solicitud en el plazo de 10 días a contar desde la recepción de la solicitud.

Derecho de cancelación o supresión

- Permite que se supriman los datos que resulten ser inadecuados o excesivos.
- La cancelación dará lugar al bloqueo de los datos, por lo que el comercio online no podrá realizar ninguna operación con ellos.
- Durante el plazo en el que le puedan ser exigidas responsabilidades legales, el comercio online conservará a disposición de las Administraciones Públicas, Jueces y Tribunales una copia de los datos. Transcurrido dicho plazo deberá proceder a su borrado.
- El comercio online deberá contestar a la solicitud en el plazo de 10 días a contar desde la recepción de la misma.
- Los datos necesarios para mantener la relación contractual con la tienda online no podrán ser cancelados mientras exista esa relación, como por ejemplo la suscripción a un servicio de pago.

Derecho de oposición

- Permite solicitar y conseguir que no se lleve a cabo el tratamiento de datos o se cese en el mismo. Un ejemplo muy común sería para que el comercio online cese en el tratamiento publicitario de datos personales.
- El comercio online deberá contestar a la solicitud en el plazo de 10 días a contar desde su recepción excluyendo del tratamiento los datos relativos al afectado o denegando motivadamente la misma.

A estos derechos, el 25 de mayo de 2018 se suman otros tres:

Derecho a la limitación de tratamiento

- Mediante este derecho un consumidor puede solicitar que se suspenda el tratamiento de sus datos que realice un comercio online cuando haya ejercido frente a ese comercio su derecho a la rectificación de sus datos personales.
- También puede solicitar que se suspenda el borrado de sus datos personales si los necesita para el ejercicio de acciones legales o si el tratamiento al que fueron sometidos resultó ilegal. Durante la suspensión del tratamiento los datos solo podrán ser utilizados para su almacenamiento, con el consentimiento del consumidor o para atender fines de interés público.

Derecho a la portabilidad de los datos

- Permite al usuario obtener una copia de los datos personales que le conciernan y que haya facilitado a un comercio online a fin de poder transmitirlos a otro servicio.
- Si es técnicamente posible, el usuario tiene derecho a que la tienda online transmita sus datos personales al servicio indicado por él y el comercio está obligado a ejecutarlo.

Derecho a no ser objeto de decisiones automatizadas individuales

- Un usuario de comercio online tiene derecho a no ser objeto de decisiones tomadas de forma automatizada, por ejemplo, mediante la elaboración de perfiles y que le afecten de manera significativa.
- Un comercio online podría tomar ese tipo de decisiones si es necesario en el marco del contrato que le relaciona con el usuario o si la legislación lo permite específicamente. También puede solicitar el consentimiento a sus usuarios para adoptar ese tipo de decisiones. En este caso, el interesado puede negar su autorización a que se tomen ese tipo de decisiones.

Más información en:

Links
- *Derechos LOPD*
- *¿Qué derechos tendré cuando se aplique el nuevo Reglamento?*
- *Reclamación de tutela de derechos*

3.5. DEBER DE SECRETO Y PUBLICACIÓN DE DATOS

El comercio online, así como cualquiera que en su nombre recoja o trate datos personales, está obligado a guardar secreto profesional. Esa obligación continúa incluso después de haber finalizado la relación comercial o contractual con él.

En ningún caso pueden hacerse públicos los datos personales de los visitantes y clientes de un comercio online sin su consentimiento. Su publicación en internet de forma que sea accesible sin restricciones es una violación de la normativa vigente que puede ser denunciada ante la AEPD.

Para interponer una denuncia:

- *Denuncia en la sede electrónica de la AEPD*

3.6. MEDIDAS DE SEGURIDAD Y NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD

La tienda online está obligada a adoptar medidas técnicas y organizativas que permitan garantizar a sus usuarios un nivel adecuado de seguridad. A partir del 25 de mayo de 2018, fecha de aplicación del Reglamento General de Protección de Datos, un comercio online que sufra una quiebra de seguridad que afecte a los datos personales de sus usuarios:

— Deberá comunicar a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas los detalles de la quiebra y de las medidas correctivas y preventivas adoptadas o propuestas.

— Cuando sea probable que la quiebra entrañe un alto riesgo para sus usuarios, el comercio online deberá comunicar a éstos:

- Los datos de contacto del Delegado de Protección de Datos, en su caso
- Las consecuencias de la quiebra de seguridad
- Las medidas adoptadas o propuestas para mitigar los efectos adversos y prevenir una nueva quiebra

3.7. PUBLICIDAD

Un comercio online puede enviar comunicaciones comerciales a los clientes y visitantes que hayan dado su autorización para ello.

No obstante, en el momento en que se contacta, compra o contrata con un comercio online, éste debe ofrecer al usuario la posibilidad de oponerse al envío de publicidad.

Las comunicaciones comerciales por medios electrónicos deben cumplir la normativa general publicitaria, que incluye, entre otras, la prohibición de realizar publicidad engañosa, la obligación de que la publicidad resulte identificable y la prohibición de realizar publicidad desleal. Asimismo, deberá cumplir la normativa publicitaria específica que sea de aplicación al producto o servicio promocionado. En caso de que la tienda online ofrezca una promoción sobre sus productos o servicios, deberá indicar las condiciones que aplique a dicha promoción, tales como las relativas a su duración. En caso de que realice un concurso o sorteo, se deberá facilitar un medio para acceder a las bases de participación.

Recuerda que puedes restringir la publicidad no deseada inscribiendo tus datos de forma gratuita y voluntaria en un fichero de exclusión publicitaria. Actualmente sólo existe el fichero denominado *Lista Robinson*, que está gestionado por la Asociación Española de Economía Digital (ADIGITAL).

Al inscribirte en la Lista Robinson puedes elegir el medio o canal de comunicación a través del cual no deseas recibir publicidad (correo postal, llamadas telefónicas, correo electrónico u otro medio).

Si quieres saber más:

Links · *¿Cómo evitar la publicidad no deseada?*

4. CÓMO RECLAMAR

En el caso de que finalmente se considere que se ha incumplido algún tipo de normativa, los posibles canales para reclamar serían los siguientes:

Cuando se trate de una **reclamación en materia de consumo**, los órganos competentes en esta materia, de ámbito estatal o autonómico, pueden actuar cuando se incumpla la normativa general de defensa de los consumidores y usuarios (véase el enlace *Resolución de Conflictos de Consumo*).

También resulta posible intervenir en relación con empresas que tengan su sede social en otros Estados miembros de la UE a través del Centro Europeo del Consumidor, adscrito a la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN), que forma parte de la Red-CEC creada por la Comisión Europea. Esta red, que incluye Noruega e Islandia, facilita información o asistencia en relación con la adquisición de un bien o la utilización de un servicio en un país europeo diferente al propio de residencia.

Si se trata de una **reclamación en materia de protección de datos personales**, la competente es, en principio, la Agencia Española de Protección de Datos (AEPD). La reclamación puede presentarse a través de su *Sede electrónica*. La tramitación es más ágil en los casos en que se aportan más pruebas o indicios.

Sin embargo, cuando adquirimos un bien o un servicio a distancia, a través de medios electrónicos, la protección de nuestros derechos como consumidores y usuarios está condicionada por el lugar desde el cual se nos ofrecen esos bienes o servicios. Por ello, para saber cuándo podemos acudir a las autoridades españolas y europeas debemos tener en cuenta lo siguiente:

Hasta el 24 de mayo de 2018

- Si el comerciante está establecido en España, o tiene algún establecimiento en España en el marco de cuya actividad se produzca un tratamiento de datos personales, se aplica la legislación española. Los contenidos de esta guía son plenamente aplicables, y cualquier reclamación en materia de protección de datos debe hacerse ante la AEPD.

- Si el comerciante no tiene establecimiento en España, pero está establecido en otro Estado miembro de la Unión Europea, se aplica la legislación del Estado miembro en el que tenga un establecimiento y al que dirija las actividades de su empresa. En estos casos, las reclamaciones en materia de protección de datos pueden presentarse ante la autoridad de protección de datos del Estado miembro (la lista figura al final de esta guía) o ante la AEPD, que la remitirá a la autoridad competente.

- Si el comerciante no tiene establecimiento en España ni en ningún otro Estado miembro de la Unión Europea, la AEPD sólo podrá actuar en materia de protección de datos si el comerciante utiliza en su oferta y en su relación con el potencial comprador español medios situados en nuestro país. Por ejemplo, cuando instala en los equipos terminales de los residentes en España (como ordenadores, tabletas, teléfonos inteligentes, etc.) dispositivos de almacenamiento y recuperación de datos (conocidos genéricamente como cookies).

A partir del 25 de mayo de 2018

- Lo indicado en la guía es válido cuando el comerciante tenga un establecimiento en la Unión Europea o cuando, no estando en ella establecido, ofrezca sus bienes o servicios a consumidores que residan en la Unión Europea. Las reclamaciones en materia de protección de datos pueden presentarse ante la AEPD, que dará a éstas el curso que proceda.

Finalmente, si se trata de **conductas tipificadas como delitos**, su investigación y persecución corresponde a las respectivas Fuerzas y Cuerpos de Seguridad, el Ministerio Fiscal y los correspondientes órganos judiciales.

10 CONSEJOS BÁSICOS PARA COMPRAR EN INTERNET DE FORMA SEGURA

1. Realiza tus compras en páginas que te inspiren confianza

2. Asegúrate de que en la web aparece identificado el responsable de la tienda online y su ubicación

3. Comprueba que la tienda online es segura y te proporciona toda la información que necesitas sobre consumo y tratamiento de datos personales

4. Si te es posible, utiliza una tarjeta de uso exclusivo para realizar pagos online

5. Desconfía de las ofertas demasiado atractivas, ya que podrías estar ante una web fraudulenta

6. No olvides comprobar que tus dispositivos están configurados correctamente y la conexión a internet es segura antes de proporcionar tus datos personales o tus datos de pago

7. Nunca envíes dinero en efectivo para completar una compra. Elige con cuidado el medio de pago

8. Recuerda que los comercios con sellos de confianza ofrecen mayores garantías

9. Puedes desistir de una compra o contrato sin tener que dar explicaciones en los 14 días posteriores

10. Si desistes o haces uso de la garantía, ello no debe tener coste alguno para ti, y esto incluye los gastos de envío

AUTORIDADES EN MATERIA DE CIBERSEGURIDAD, CONSUMO Y PROTECCIÓN DE DATOS

Autoridades y entidades Europeas de Ciberseguridad

- **EUROPOL**
- *Centros de Respuesta ante Incidentes de Seguridad de la Información acreditados por la red europea* **TF-CSIRT.** Trusted Indroducer.
- *European Union Agency for Network and Information Security* **(ENISA)**

Autoridades y Entidades nacionales de Ciberseguridad

- *Policía Nacional - Brigada de Investigación Tecnológica* **(BIT)**
- *Guardia Civil - Grupo de Delitos Telemáticos* **(GDT)**
- *Centro Nacional de Protección de Infraestructuras Críticas* **(CNPIC)**
- *Instituto Nacional de Ciberseguridad* **(INCIBE)** y *el CERT de Seguridad e Industria* **(CERTSI)**
- *Centro Criptológico Nacional* **(CCN-CERT)**

Autoridades Europeas de Consumo

- *Organismo europeos para la Resolución alternativa de litigios* **(RAL)**

Autoridades Europeas de Protección de Datos

- **España**

https://www.agpd.es

- **Austria**

http://www.dsb.gv.at

- **Belgica**

http://www.privacycommission.be

- **Bulgaria**

http://www.cpdp.bg

- **Croacia**

http://www.azop.hr

- **Chipre**

http://www.dataprotection.gov.cy

- **Republica Checa**

http://www.uoou.cz

- **Dinamarca**

http://www.datatilsynet.dk

- **Estonia**

http://www.aki.ee/en

- **Finlandia**

http://www.tietosuoja.fi/en

- **Francia**

http://www.cnil.fr

- **Alemania**

http://www.bfdi.bund.de

- **Grecia**

http://www.dpa.gr

- **Hungría**

http://www.naih.hu

- **Irlanda**

http://www.dataprotection.ie

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

- **Italia**
http://www.garanteprivacy.it
- **Letonia**
http://www.dvi.gov.lv
- **Lituania**
http://www.ada.lt
- **Luxemburgo**
http://www.cnpd.lu
- **Malta**
http://www.dataprotection.gov.mt
- **Países Bajos**
https://autoriteitpersoonsgegevens.nl
- **Polonia**
http://www.giodo.gov.pl
- **Portugal**
http://www.cnpd.pt
- **Rumania**
http://www.dataprotection.ro
- **Eslovaquia**
http://www.dataprotection.gov.sk
- **Eslovenia**
https://www.ip-rs.si
- **Suecia**
http://www.datainspektionen.se
- **Reino Unido**
https://ico.org.uk

Instituciones Europeas

- **European Data Protection Supervisor**
http://www.edps.europa.eu

Compra segura en INTERNET

GUÍA PRÁCTICA