Guía sobre seguridad y privacidad en el Comercio Electrónico

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Enero 2010

El **Instituto Nacional de Tecnologías de la Comunicación** (INTECO), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones en las siguientes líneas estratégicas: Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Más información: www.inteco.es

ÍNDICE

1 INTRODUCCIÓN Y DATOS SOBRE COMERCIO ELECTRÓNICO

Los cambios generados en los hábitos de los consumidores debido a la incorporación de Internet han permitido establecer nuevas relaciones entre usuarios y vendedores mediante el comercio electrónico.

Sin embargo, ello ha supuesto nuevos retos para los consumidores que adquieren bienes y contratan servicios a través de la Red, debido fundamentalmente a que las compras que se realizan en Internet no tienen las mismas características que aquellas realizadas en el comercio tradicional.

La Organización Mundial del Comercio define el comercio electrónico como la producción, promoción, venta y distribución de productos a través de redes de telecomunicación.

El comercio electrónico permite el acceso a un mercado global y competitivo, que genera numerosas ventajas para los ciudadanos entre las que destacan la reducción de precios así como el acceso a nuevos productos. Sin embargo a pesar de las ventajas que el comercio a través de Internet ofrece, existen todavía reticencias y miedos a comprar en la Red. Dichos miedos se centran fundamentalmente en problemas de seguridad que justifican el rechazo a las compras electrónicas.

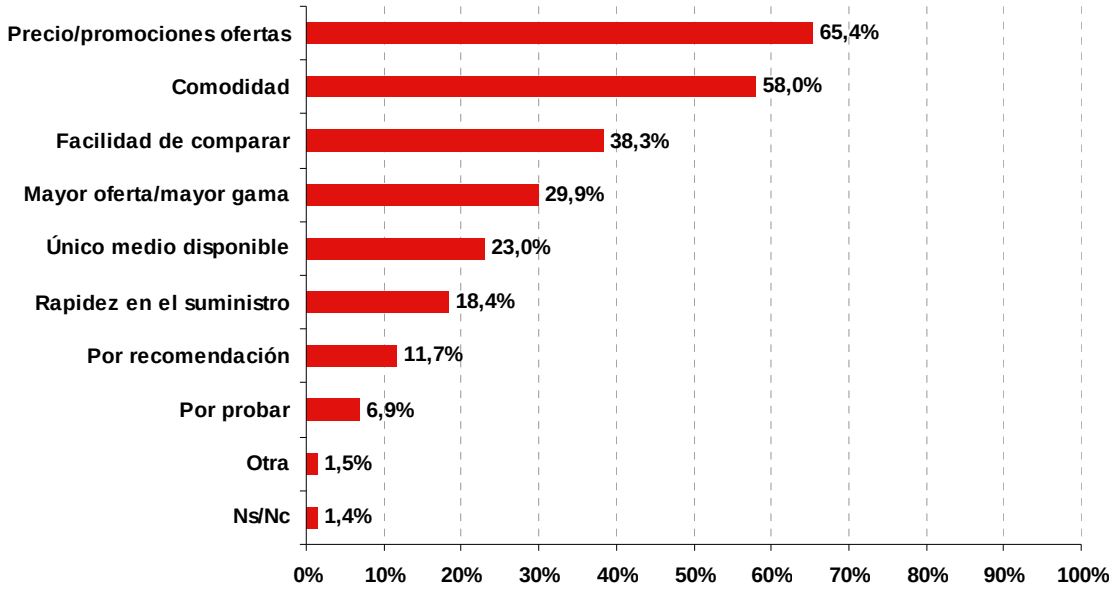
Por ello es necesario informar sobre la legislación aplicable al comercio electrónico de modo que el consumidor conozca cual es la protección que se le confiere.

El objeto de la presente guía es ayudar al ciudadano a realizar operaciones de comercio electrónico en Internet de forma segura, de modo que se minimicen los riesgos de dichas operaciones. A tal fin se examinarán las fases de la contratación electrónica, los derechos del consumidor, la solución de conflictos de consumo así como las diferentes amenazas y vulnerabilidades que pueden afectar a los sistemas.

En 2009 se alcanzó la cifra de 10,4 millones de individuos que realizaron compras a través de Internet, un incremento del 17% con respecto al año anterior debido al aumento del número de internautas y de su uso del comercio online. Entre las razones de esta

preferencia por el canal online destacan los mejores precios (65,4%), la comodidad (58,0%) o la facilidad para comparar con otros productos (38,3%)[1].

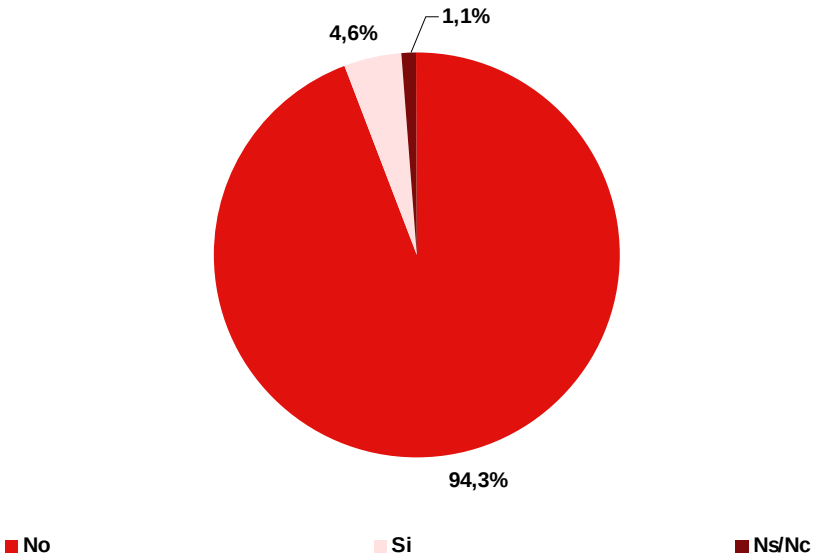
Gráfico 1: Principales razones por las que ha comprado en 2009 productos/ servicios a través de Internet en lugar de acudir a una tienda física (%)



Fuente: Observatorio Red.es

La gran mayoría de internautas (94,3%) manifiesta que no ha percibido ningún problema a la hora de realizar adquisiciones a través de Internet.

Gráfico 2: ¿Ha tenido alguna vez problemas en las compras realizadas por Internet en el año 2009 y 2008? (%)



Fuente: Observatorio Red.es

[1] Estudio sobre Comercio Electrónico B2C 2010 – ONTSI. Disponible en : http://www.red.es/media/registrados/2010-11/1288789343549.pdf?aceptacion=4fd29730af61d6052e69bc17db191048

En cuanto a los usuarios que han sufrido algún problema en sus compras online, se ha producido un incremento en las reclamaciones y aproximadamente dos de cada tres usuarios reclaman frente a incidencias en la compra. En la Tabla 1 se aprecia el organismo sobre el que los usuarios realizan la queja y el tiempo en el que se resuelve su resolución. La mayoría de usuarios (90,3%) reclaman ante el servicio de atención al cliente de quien les vendió el producto. En cuanto al tiempo, el 72,4% de las reclamaciones se resuelven en el plazo máximo de un mes. Solo un 5,9% de las reclamaciones finalmente no se resuelve.

Tabla 1: Organismo ante el que el usuario efectuó la reclamación y tiempo en el que se resolvió la reclamación (%)

Organismo ante el que efectuó la reclamación	
Al servicio de atención al cliente de quien le vendió el producto/servicio	90,3
Paypal	-
Queja a algún organismo de la Administración Pública.	4,4
Queja a alguna Asociación de usuarios.	-
Otras	5,3
Tiempo en el que se resolvió la reclamación	
Menos de una semana	26,4
Una semana a un mes.	46,0
Más de un mes.	21,7
No se resolvió.	5,9

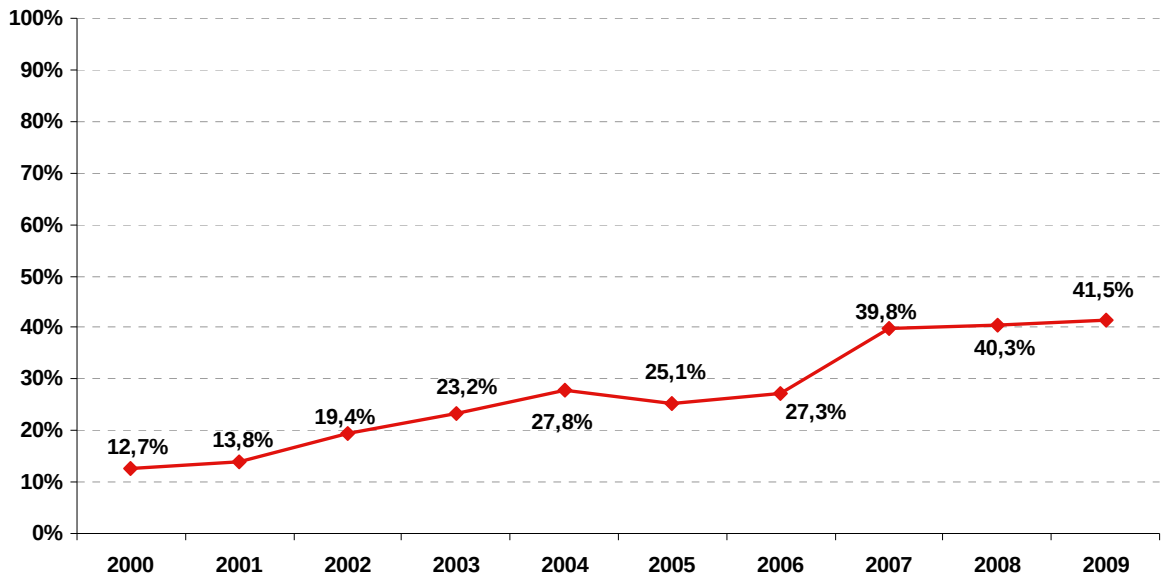
Fuente: Observatorio Red.es

El volumen de negocio generado por el comercio electrónico B2C (dirigido al consumidor) en 2009 superó los 7.700 millones de euros, lo que supuso un incremento del 15,9% respecto a 2008.[2]

El porcentaje de internautas que realiza compras a través de Internet se incrementa ligeramente pasando de un 40,3% a un 41,5% del total de internautas de 2008 a 2009. Se puede deducir que el principal motor del aumento del número de compradores se basa principalmente en la ampliación de la población internauta.

[2] Op. cit 1

Gráfico 3: Evolución del número de internautas compradores (%)



Fuente: Observatorio Red.es

Las principales compras que realizan los internautas son reservas de alojamientos (46,7%), billetes de transporte (40,0%) y alquiler de coches (36,6%), reflejo de la notable importancia del comercio electrónico sobre el sector del turismo.

Por detrás de este sector, los sectores que mayores porcentajes de compra online registran son el sector de la tecnología (el 34,4% de los internautas adquiere servicios de Internet y el 20,9% software) y el del ocio (la compra de entradas en el canal online supone el 23% mientras que los productos multimedia en formato digital –DVD, música, videojuegos, etc.- el 21,6%).

2 BENEFICIOS Y OPORTUNIDADES DEL COMERCIO ELECTRÓNICO

A través del comercio electrónico se posibilita que los usuarios accedan a un mercado lleno de oportunidades desde su ordenador personal. Estas oportunidades llevan consigo tanto una serie de ventajas como de inconvenientes.

Ilustración 1: Ventajas e inconvenientes del comercio electrónico

2.1 VENTAJAS DEL COMERCIO ELECTRÓNICO

2.1.1 Mercado abierto 24h 365 días al año

La Red permite realizar compras durante todos los periodos del año con independencia de las imposiciones de los distintos horarios comerciales.

2.1.2 Acceso a múltiples productos

El comercio electrónico permite acceder a un mercado mundial. Posibilitando el acceso a productos, por ejemplo, que no se encuentren a la venta en el país de residencia del usuario.

Aunque es necesario tener en cuenta las restricciones que ponen determinadas empresas a la hora de comercializar productos que no se encuentran en las tiendas físicas del país desde el que se realiza la petición o tienen áreas de reparto geográficas limitadas (garantía, soporte, etc).

2.1.3 Productos más económicos

La existencia de una competencia global, la venta directa al consumidor, la reducción de márgenes, etc., son factores que afectan al precio de los productos en Internet, permitiendo disminuir el mismo con respecto a su valor en el comercio tradicional.

2.1.4 Feedback de los usuarios

Foros, blogs, páginas especializadas en productos, son herramientas que la Red ofrece de cara a elegir el mejor producto posible de acuerdo a los criterios del comprador. De esta manera, la puesta en común de diferentes opiniones y experiencias permite elegir el producto más adecuado de acuerdo con las necesidades del consumidor.

2.1.5 Oferta de servicios personalizada

Las múltiples oportunidades que ofrece el comercio electrónico, permiten personalizar y configurar los productos en función de las necesidades del usuario.

2.1.6 Comodidad y agilidad en las compras

La posibilidad de acceder a los productos desde cualquier lugar permite al ciudadano evitar colas y desplazamientos sin necesidad de salir de su hogar.

2.1.7 Comparación de productos

La existencia de páginas especializadas en la comparación de productos, la posibilidad de equiparar precios y calidades entre las diferentes marcas o comercios en Internet, sin necesidad de cambiar de ubicación es otra de las grandes ventajas del comercio electrónico.

2.1.8 Soporte Online

La existencia de servicios de ayuda online durante las 24 horas del día son herramientas de valor añadido que los vendedores ofrecen. Estas permiten incrementar de manera notable la e-confianza el ciudadano deposita en el comercio electrónico.

2.2 INCONVENIENTES DEL COMERCIO ELECTRÓNICO

2.2.1 Falta de contacto físico con el producto

Las transacciones que se realizan a través de Internet son de carácter no presencial, lo que genera un cierto grado de incertidumbre. A su vez se omite tanto la atención personal como el contacto físico con el artículo, factores que pueden influir de forma determinante en la elección de un producto u otro.

En el caso del comercio electrónico, a fin de eliminar dicha desventaja se está produciendo la incorporación de chats en directo o asistentes virtuales que ayudan a resolver dudas durante el proceso de compra.

2.2.2 Falta de seguridad y fiabilidad

Es un punto clave a la hora de decidir la compra a través de Internet que la empresa esté bien identificada y sobre todo que ofrezca la posibilidad de contactar directamente con ella.

También es vital que disponga de información clara, completa y concisa tanto sobre temas contractuales como sobre el producto/servicio y el precio, clarificando los gastos que van o no incluidos en la transacción.

2.2.3 Problemas de distribución

Las incidencias logísticas (retrasos en la recepción, recepción del pedido con desperfectos, no recibir el producto) son otro de los principales inconvenientes del comercio electrónico.

2.2.4 Problema de reclamaciones y devoluciones

La principal problemática en las compras a través de la Red es que el producto o servicio adquirido no responda a lo que se ofrecía en Internet. La inseguridad de a quien dirigirse en caso de reclamación es otro de los problemas que conlleva el comercio electrónico.

2.2.5 Problemas de pago

En la mayoría de los casos, las compras a través de Internet se realizan utilizando el número de la tarjeta de crédito del comprador, pero aún no es 100% seguro introducirlo en la Red sin conocimiento alguno.

3 FORMAS DE COMERCIO ELECTRÓNICO

3.1 B2C: COMERCIO DE EMPRESA A CLIENTE

El término viene de la expresión inglesa *Business To Customer* (Desde el Negocio al Consumidor).El concepto abarca todas las acciones y pasos necesarios para que la empresa ponga el producto directamente en manos del consumidor final mediante medios electrónicos online.

3.2 B2B: COMERCIO DE EMPRESA A EMPRESA

En este caso el término viene de la expresión inglesa *Business To Bussines* (Desde el Negocio al Negocio, o comercio de empresa a empresa).

Engloba las transacciones a través de Internet realizadas entre dos o más empresas, por ejemplo, fabricante, distribuidor y negocio final, pero no incluye en ningún caso en la cadena al consumidor final.

En particular agrupa todas las acciones del proceso para que la empresa ponga el producto al final de la cadena de venta y a disposición del último paso antes de llegar al consumidor final.

Las categorías B2C y B2B representan en la actualidad la mayor parte del comercio a través de la Red.

3.3 B2E: COMERCIO DE EMPRESA A SUS TRABAJADORES

El término procede de la expresión inglesa *Business To Employee* (Desde el Negocio hacia el Empleado), donde la empresa ofrece a través de su portal para empleados, servicios o ventajas a sus trabajadores de otros servicios que no constituyen el principal de la empresa. Por ejemplo ofreciendo ventajas en viajes o alquiler de vehículos.

3.4 B2B2C: COMERCIO DE EMPRESA A EMPRESA Y A CLIENTES

Es la unión de los casos de B2B y B2C. Este sistema se basa en la utilización de plataformas en Internet para agrupar los procesos de distribución desde la fabricación y distribución hacia el consumidor y poner el producto en sus manos, siendo éstos últimos o bien empresas o bien consumidores domésticos.

Existen también otras categorías menos frecuentes como *Bussines To Goverment* (De Gobierno a Empresa, o al revés, De Empresa a Gobierno).

El comercio electrónico forma a su vez parte de un concepto más amplio como es del de negocio electrónico (e-Business) el cual engloba los procesos de marketing y compra-venta de productos y/o servicios a través de Internet.

4 CUMPLIMIENTO NORMATIVO

El comercio electrónico afecta a numerosos aspectos legales, protección de datos personales, seguridad en transacciones, legalidad de comercio interior, publicidad de productos y servicios, garantía y protección de los consumidores.

Las principales normas que afectan a la seguridad en el comercio electrónico son analizadas a continuación.

4.1 PRESTACIÓN DE SERVICIOS DE COMERCIO ELECTRÓNICO

4.1.1 Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)

La LSSICE regula aspectos determinantes del comercio electrónico en el mercado interior, aplicándose con carácter general a las empresas establecidas en España.

- **Obligaciones que impone la LSSICE**

  Entre las obligaciones para los Prestadores de Servicios de la Sociedad de la Información que incluye la Ley se encuentran, entre otras:

  - Información general: nombre o denominación social, datos de inscripción en el registro, etc.
  - Deber de colaboración de los prestadores de servicios de intermediación.
  - Obligaciones de información sobre seguridad.

4.1.2 Ley de Ordenación del Comercio Minorista para las ventas a distancia y art. 4.2 de la Directiva sobre ventas a distancia.

La Ley 7/1996, de 15 de Enero, establece que la oferta de venta a distancia debe incluir:

- Identidad del proveedor.
- Características especiales del producto.
- Precio y, en su caso, debidamente separados, los gastos del transporte.
- Forma de pago y modalidades de entrega o de ejecución.
- Plazo de validez de la oferta.

Otras características de la Ley son:

- En ningún caso la falta de respuesta a la oferta de venta a distancia podrá considerarse como aceptación de aquélla.
- Queda prohibido enviar al consumidor o usuario artículos o mercancías no pedidas por él al comerciante, exceptuándose las muestras comerciales.
- Cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo.

El contenido mínimo que debe suministrarse al consumidor se recoge en el art. 4.2 d la Directiva 1997/7/CE. Ésta no es otra que identidad del prestador de servicios, características esenciales de la prestación, precio del producto, gastos de entrega, etc.

4.2 PROTECCIÓN DE DATOS

4.2.1 Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (RLOPD)

La empresa de acuerdo con lo dispuesto en esta Ley tiene la obligación de proporcionar la siguiente información al cliente antes de que envíe los datos:

- Acerca de la existencia de un fichero o tratamiento de datos de carácter personal.
- Finalidad de la recogida.
- Destinatario de la información.
- Carácter obligatorio o facultativo de las respuestas.
- Posibilidad de ejercitar derechos de acceso, rectificación, cancelación, y oposición.
- Identidad y dirección del responsable.

Ese tipo de información se suele proporcionar al usuario en un enlace denominado Política de Privacidad que suele situarse en la parte inferior del portal de la empresa.

A su vez mediante la LOPD se establece la obligación de las empresas de adoptar medidas de seguridad que garanticen la seguridad y secreto a la vez que se realiza la inscripción en el Registro General de Protección de Datos.

4.3 DEFENSA DE CONSUMIDORES Y USUARIOS

4.3.1 Real Decreto Legislativo 1/2007 de 16 de Noviembre por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias

Recoge los derechos básicos de los consumidores y usuarios entre los que se encuentran:

- El derecho a recibir información previa sobre los bienes y servicios objeto del contrato.
    - Amplía lo dispuesto en la Ley 34/2002 (LSSICE) obligando a las empresas de comercio electrónico a especificar en la web, la forma de pago, las modalidades de entrega, y la existencia de un derecho de desistimiento o renuncia a la compra realizada.
- El derecho de desistimiento unilateral en la contratación electrónica.
    - Según el mismo el consumidor tiene derecho a renunciar a la compra efectuada en un plazo de 7 días hábiles sin penalización alguna y sin la necesidad de indicar los motivos por los que rechaza la compra (el prestador del servicio podrá ampliar dicho plazo pero nunca reducirlo o eliminarlo).
    - El comprador no tendrá que soportar coste alguno salvo el coste directo de la devolución del producto.
- El derecho a una indemnización de daños y perjuicios por los daños sufridos o la protección en situaciones de inferioridad o vulnerabilidad.
- La obligación para el vendedor de devolver en su totalidad el precio del producto en caso de falta de conformidad. Así como la regulación de la exigencia de sustitución o reparación de los productos no conformes con el contrato, acciones que serán gratuitas para el consumidor y usuario, incluidos los gastos de envío.

5 AMENAZAS EXISTENTES EN EL COMERCIO ELECTRÓNICO

Las amenazas concretas hacia el comercio electrónico se dirigen especialmente hacia los datos sensibles del usuario, con el fin de comprometer la seguridad, a nivel económico, técnico y personal. De ellas, el phishing o fraude a través de Internet es la principal amenaza del comercio electrónico.

5.1 PHISHING

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

El estafador o *phisher* suplanta la identidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

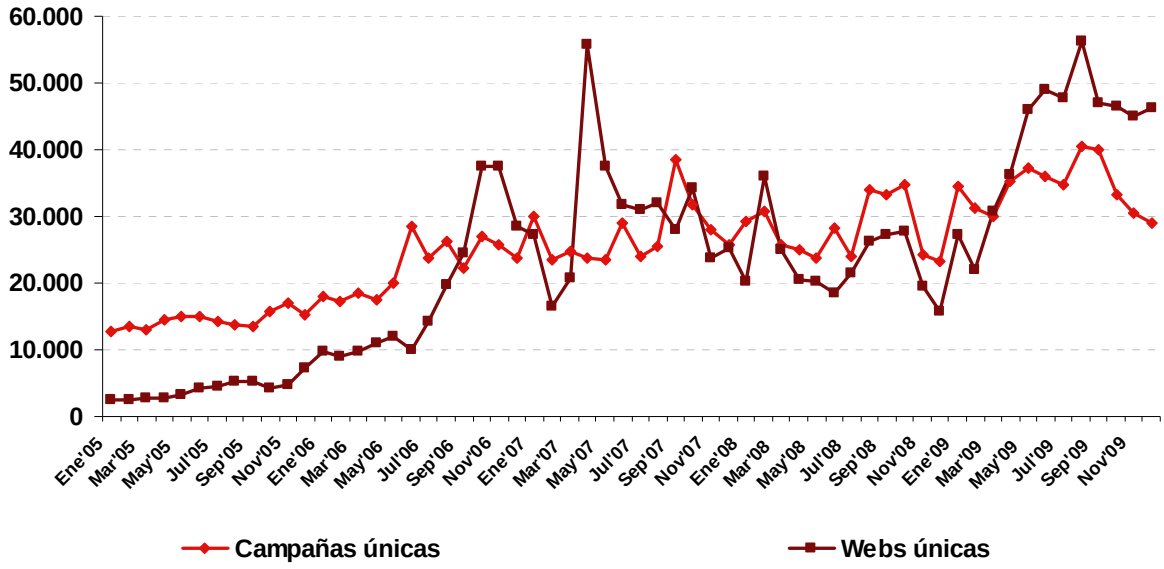
El phishing incluye el envío de correos electrónicos falsos, procedentes, en apariencia, de empresas o entidades legítimas (por ejemplo entidades bancarias o páginas de compra online o de subastas), y dirigen al destinatario a webs falsas que replican las de la empresa o entidad legítima. La intención de dichos correos cuando se dirigen a clientes de entidades financieras es intentar que estos revelen sus datos personales o bancarios: número de tarjeta de crédito, claves de acceso (PIN), contraseñas para operar, u otro tipo de datos confidenciales y personales.

El phishing es un fenómeno cuya magnitud y transcendencia es mayor cada día. Según el *Anti Phising Working Group* (APWG), en diciembre de 2009 se crearon 46.190 sitios web fraudulentos, y se realizaron 28.897 campañas de fraude únicas.

El fraude a través de Internet es un fenómeno global: en la actualidad se detectan entorno a 50.000 nuevas webs fraudulentas cada mes distinguiéndose:

- **Campañas únicas de phishing**, que el APWG define como cada e-mail dirigido a varios usuarios, apuntando a una misma página web, con un mismo asunto en el correo electrónico.
- **Webs únicas de phishing**, URLs fraudulentas.

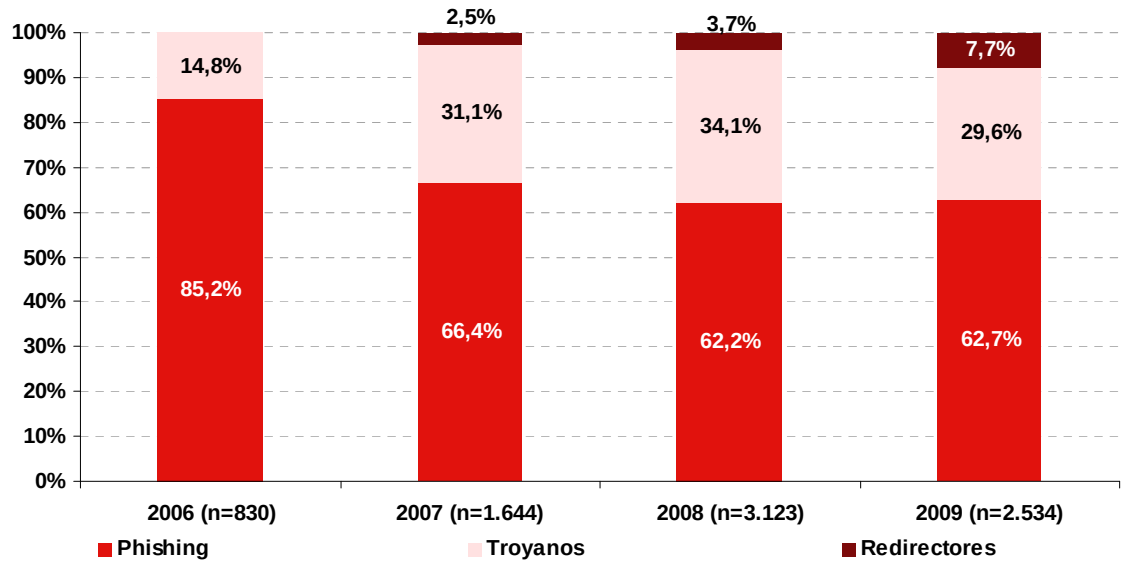
Gráfico 4: Evolución del phishing entre 2005 y 2009



Fuente: Anti-Phishing Working Group (APWG)

El siguiente gráfico profundiza en la evolución de los distintos tipos de fraude online dirigidos a entidades en España. La proporción en que phishing, troyanos y redirectores se posicionan dentro de ese total se modifica porque los dos segundos experimentan una tendencia creciente en los últimos años frente al phishing.

Gráfico 5: Evolución de los distintos tipos de fraude en Intenet dirigidos a entidades españolas (%)



Fuente: S21sec

5.2 CÓDIGOS MALICIOSOS -MALWARE-

Se aprecia una nueva tendencia que refleja que las técnicas de fraude a través de Internet se están desplazando, desde aquellas basadas en la ingeniería social, hacia aquellas que se basan en la inyección de código malicioso o malware.

Dicho cambio de tendencia es fruto de la mayor concienciación ciudadana sobre la seguridad, de ahí que haya aumentado la cautela de los ciudadanos a la hora de facilitar sus datos personales, y se utilicen otros métodos más allá del engaño para recoger la información de los usuarios.

El malware presente en los equipos pretende, por ejemplo, robar los datos bancarios de los usuarios, utilizando, entre otros, sistemas que interceptan clave de usuario y contraseña o programas que corrompen las infraestructuras de navegación y redirigen a los usuarios a webs falsas.

5.3 OTROS TIPOS DE AMENAZAS

Existen amenazas con un carácter más técnico distintivas del comercio electrónico:

5.3.1 *Carding* y *Skimming*

Consisten en el uso fraudulento de tarjetas (*carding*) y la copia de las bandas magnéticas (*skimming*).Ello permite el acceso a cuentas bancarias, a números de tarjeta robados, a vuelcos de bandas magnéticas así como a perfiles personales.

Una vez que se tiene acceso a dichos datos se procede a su venta. Así los datos de una cuenta con un saldo de 30.000€ pueden alcanzar en dichos mercados 2.200€ con el fin de ser explotada posteriormente por el adquiriente de dichos datos.

Tabla 2: Datos de cuentas bancarias en venta, tomados de un sitio Web de carding

Nombre del banco	País	Saldo	Precio
Bank of América	EE.UU.	…..	Vendido
Asmouth Bank	EE.UU.	16.040 $	700 €
Washington Mutual bank	EE.UU.	14.400 $	600 €
Washington Mutual bank	EE.UU.	7.950 $ + 2.612 £	500 €
Washington Mutual bank	EE.UU.	….	Vendido
MBNA America Bank	EE.UU.	22.003 $	1.500 €
Banco Bradesco S.A.	Brasil	13.451 $	650 €
Citibank	Reino Unido	10.044 £	850 €
NatWest	Reino Unido	12.000 £	1.000 €
BNP Paribas	Francia	30.792 €	2.200 €
Caja de Ahorros de Galicia	España	23.200 €	1.200 €
Caja de Ahorros de Galicia	España	7.846 €	500 €
Banco Sabadell	España	25.663 €	1.450 €

Fuente: PhishTank

5.3.2 *Pharming*

Mediante un troyano[3] es posible que un atacante se infiltre entre la dirección IP y el nombre del servidor al que responde. Es una técnica sumamente peligrosa dado que la víctima cree estar visitando un sitio web legítimo.

Según las estadísticas mensuales de *phistank*[4] en diciembre de 2009, el objetivo más popular fue *PayPal*.

[3] Los caballos de Troya o troyanos son los principales programas maliciosos relacionados con el comercio electrónico. Parecen inofensivos a primera vista, pareciendo ser útiles, pero dicho programa expondrá el ordenador a atacantes, abriendo lo que se conocen como "puertas traseras" o vías de acceso al equipo sin el consentimiento del usuario. Esto provoca que la máquina quede desprotegida, permitiendo que le roben información sensible y/o tomar el control remotamente de ella

[4] Estadísticas de abril de 2009: http://www.phishtank.com/stats/2009/04/

Tabla 3: Objetivos más populares de los ataques de phising

Objetivos	Ataques de phishing válidos en diciembre 2009
PayPal	12.663
Tibia	853
JPMorgan Chase and Co.	727
Sulake Corporation	628
Facebook	507
Internal Revenue Service	424
HSBC Group	144
Bank of America Corporation	114
Google	101
Nedbank Ltd.	82

Fuente: PhishTank

5.3.3 *Crimeware*

Incluyen ladrones de contraseñas, capturadores de pulsaciones que registran los datos del teclado, realizan capturas de video, o toman imágenes de la pantalla y envían los datos a los sitios de recogida.

El *crimeware* suele estar asociado con *rootkits* (programas maliciosos que ocultan el *crimeware* y lo hacen invisible para muchas herramientas de seguridad). Esta forma de ataque se está especializando en ataques selectivos, introduciéndose en los ordenadores que visitan webs fraudulentas y eludiendo la detección por parte de los antivirus salvo que sean capaces de identificarlos de forma genérica o mediante análisis del comportamiento.

5.3.4 *Clickjacking*

Esta técnica, conocida también por secuestro de clic es una vulnerabilidad que afecta a navegadores y otros productos web.

Mediante esta técnica un atacante puede forzar al equipo del usuario a hacer click en cualquier vinculo o link de una web, pudiendo dirigir la navegación hacia webs con virus, troyanos o anuncios no deseados, sin que el usuario se de cuenta de lo que está ocurriendo. Por ello es fuente potencial de ejecución de phishing, basándose en pulsaciones no voluntarias del ordenador del usuario sobre enlaces comerciales en webs.

6 HERRAMIENTAS DE PROTECCIÓN Y SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Para combatir amenazas como el phishing o el código malicioso que infecta a los equipos de los internautas, existen distintos medios a disposición de los usuarios. A continuación se presentan medidas y herramientas de carácter técnico.

6.1 MÉTODOS SEGUROS DE PAGO POR INTERNET

Los principales métodos de pago para realizar operaciones a través de la Red son el pago con tarjeta de crédito, el método contra reembolso, la transferencia bancaria o el pago mediante intermediarios (por ejemplo, mediante *Paypal*).

6.1.1 Pago con tarjeta

En este sentido, el pago con tarjeta de crédito o débito es un sistema rápido que ofrece seguridad y garantías, ya que si el usuario recibe un cargo fruto de una equivocación o fraude, dispone de tres meses para anularlo.

Así mismo, con el objeto de fomentar la e-confianza en las compras en Internet, la mayoría de las entidades bancarias ponen a disposición de sus clientes tarjetas específicas para la compra en la Red. Son denominadas tarjetas de pago online para compras por Internet o tarjetas prepago; se encuentran disponibles en las oficinas de todas las entidades bancarias y su funcionamiento es idéntico al de las tarjetas habituales. Su responsabilidad sólo se subscribe a la cantidad de dinero con la que el cliente carga la tarjeta (que puede ser cualquier cantidad que él desee), y sólo sirven para realizar compras por Internet o, en algunos casos, también para comprar en los comercios habituales.

Para hacer frente a los fraudes en el comercio electrónico las redes de *Visa* y *MasterCard* establecieron una norma concebida para proteger a los titulares de tarjetas cuando compran por Internet. La norma relativa a la seguridad de los datos del sector de las tarjetas de pago, PCI DSS (*Payment Card Industry Data Security Standard*), permite mejorar la seguridad de las transacciones y el almacenamiento de datos bancarios.

6.1.2 Pago contra-reembolso

Consiste en pagar en efectivo en el momento de recibir la compra en el punto de entrega. No es necesario proporcionar datos bancarios en la páginas de compra, aunque sí datos de dirección postal. En algunos casos genera recargos por un importe de un porcentaje de la compra con respecto al pago.

6.1.3 Transferencia bancaria

Consiste en ingresar el importe de la compra en la cuenta del vendedor mediante una operación bancaria. La ventaja principal que presenta este método de pago es la no revelación de los datos asociados a la cuenta corriente. Sin embargo, a diferencia del pago con tarjeta, si éste se realiza por adelantado se pierde cualquier opción a cancelar dicho envío si la compra no resulta satisfactoria.

6.1.4 Pago mediante intermediarios

En la Red existen intermediarios que permiten evitar tener que facilitar los datos bancarios a un vendedor desconocido, que es lo que sucede cuando se paga mediante tarjeta de crédito a una empresa en la Red que no dispone de una pasarela de pago con una entidad bancaria.

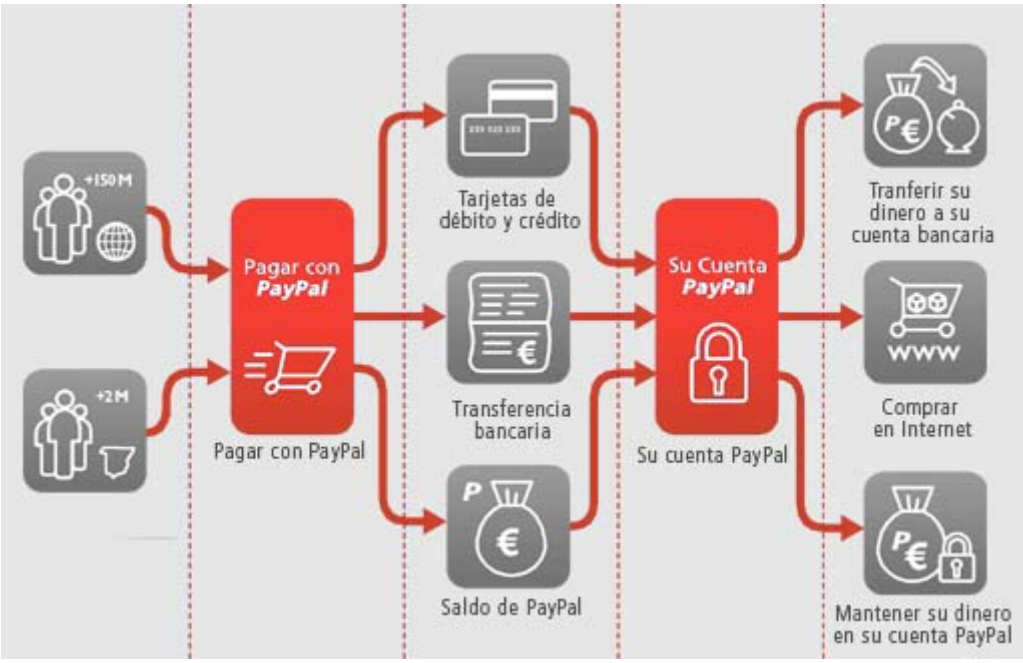


Ilustración 2: Funcionamiento PayPal

Mediante los intermediarios estos datos no se facilitan al proveedor, sino a un tercero de confianza que actúa de intermediario financiero, de manera que es éste el que procede al pago al vendedor. De dicho modo los datos de la tarjeta bancaria se encuentran únicamente en una empresa intermediaria de confianza de forma que el vendedor no conoce nunca los datos reales de la tarjeta o cuenta corriente.

El ejemplo más conocido y utilizado de intermediario financiero es *PayPal*, pero también existen otros intermediarios financieros como pueden ser los casos de *Google Checkout* o *Amazon Payments*.

6.1.5 Pago a través de domiciliación bancaria

Consiste en domiciliar los pagos de compras de forma periódica o la contratación de servicios continuados, al igual que se realiza con los pagos de servicios como la electricidad o el agua.

Con el fin de protegerse ante riesgos innecesarios, es necesario contar con un sistema de notificaciones que permita al comprador conocer cuándo el vendedor ejecuta el cargo en la cuenta bancaria facilitada. Así, cuando dicho cargo es notificado al comprador, y en función de los acuerdos que el comprador tenga con la entidad bancaria, se establece un periodo de tiempo en el que puede reclamar para que dicho cargo sea anulado.

6.2 PASOS PARA REALIZAR UNA COMPRA SEGURA

Para ejecutar una compra segura a través de la Red deben llevarse a cabo los siguientes pasos:

Ilustración 3: Pasos para realizar una compra segura en Intenet

6.2.1 Utilizar un ordenador personal

En primer lugar se debe **utilizar un ordenador personal, y no uno de acceso público**. Los niveles de seguridad en un ordenador personal bien configurado suelen ser superiores a los que ofrecen los ordenadores de acceso público. Es uno de los motivos por los que la mayoría de compras de productos de comercio electrónico se deben realizan en el hogar.

En el caso en que se realice la compra al que posteriormente puedan tener acceso otras personas, al finalizar la compra se debe recordar:

- Eliminar las cookies.
- Eliminar los archivos temporales del navegador web.
- Cerrar la sesión de usuario de los servicios a los que haya tenido acceso en esa sesión o de la oficina virtual de la entidad.

6.2.2 Comprobar que el ordenador es seguro

El siguiente paso es comprobar que el ordenador desde el que se realiza la compra es seguro. Es recomendable tener un ordenador libre de amenazas a fin de realizar operaciones de comercio electrónico de forma segura. Para ello la Oficina de Seguridad del Internauta (OSI) pone a la disposición del usuario un conjunto de consejos y recomendaciones que se pueden resumir en:

- **Actualizaciones de software**: mantener actualizado el equipo, tanto el sistema operativo como cualquier aplicación que esté instalada, incluido el navegador, para que los códigos maliciosos no puedan encontrar un punto débil en el equipo. Igualmente se deben activar las actualizaciones automáticas.

- **Utilizar software con licencia** que ofrezca garantía y soporte.

- **Cuentas de usuario**: utilizar siempre una cuenta de usuario con privilegios limitados para realizar comercio electrónico.

- **Herramientas**: es imprescindible tener instalado:

  - Un programa antivirus de escritorio y además utilizar ocasionalmente un antivirus en línea.

  - Un programa cortafuegos.

  - Un programa anti-espía de escritorio y utilizar ocasionalmente uno en línea para navegar por Internet

- Es recomendable **tener instalados otros programas de seguridad** como analizadores de URL: permiten categorizar las páginas a las que se accede a fin de determinar el grado de confianza de las mismas.

- Utilizar contraseñas robustas y seguras en todos los servicios que se utilicen, cambiándolas periódicamente y sin revelarlas a nadie, ni anotarlas en lugares visibles o de fácil acceso como pantallas, teclados o crear documentos de texto que contengan dichas claves.

- Realizar una **navegación segura** en Internet:

  - Como se expondrá con más detalle más adelante se debe utilizar una autenticación segura: al introducir el usuario y contraseña la información debe ir cifrada, para cerciorarse de ello es necesario asegurarse que durante el proceso la dirección de la página comience por “https://”, especialmente en ordenadores públicos.

- Configurar su navegador para que sea seguro.
- Analizar con un programa antivirus todo archivo que se descargue de Internet.
- Configurar el correo electrónico de modo seguro: utilizando un filtro anti-spam y no abriendo ficheros sospechosos de fuentes desconocidas.

6.2.3 Verificar la legitimidad de la web

El siguiente paso para realizar una compra segura consiste en verificar la legitimidad de la web de compra y comprobar que es segura.

Para ello, el art. 27 de la Ley 34/2002, de 11 de Julio, modificada por la Ley 56/2007 establece el principio de previo consentimiento informado, según el cual toda la información que se suministre debe aparecer en la pantalla de manera clara, compresible e inequívoca (art. 40.2 LOCM) y fácilmente identificable por parte del consumidor, por lo que, los iconos o enlaces bajo los cuales se oculte la información, han de ser lo suficientemente expresivos del contenido. Dichos enlaces suelen encontrarse en la parte inferior de la web.

El primer paso es identificar al vendedor, para lo que es necesario buscar en la página web la identidad de la empresa

Identificar la oferta comercial. El art. 20 Ley 34/2002 modificada por la Ley 56/2007 establece que en todas las propuestas de contratación deberá constar inequívocamente que se trata de una oferta de contrato y no de una mera comunicación publicitaria.

En particular:

- Se debe verificar la legitimidad del sitio web: los atacantes intentarán engañar mediante correos electrónicos y páginas web que suplantan la identidad del banco o comercio. Es necesario aprender a reconocer páginas web y mensajes fraudulentos, para que esto no ocurra.
- A su vez se puede utilizar como apoyo los filtros antifraude de los navegadores diseñados para alertar al visitar una página fraudulenta y siempre manteniendo el navegador con una configuración segura.

- Si es la primera vez que se utilizan los servicios en línea de una entidad desconocida, se han de tener en cuenta los siguientes consejos para identificar una entidad de garantías:

    - Informarse sobre el sitio antes de comprar: desconfiar de empresas que ofrecen precios demasiado bajos o que no facilitan dirección física y teléfono de contacto. Si estos datos están disponibles, es conveniente comprobar la existencia de la dirección o utilizar el teléfono para comprobar que el establecimiento existe.

    - Leer la Política o Declaración de Privacidad del sitio, ya que todas las empresas que ofrecen sus productos en Internet deben ofrecer información sobre el tratamiento que van a dar a sus datos personales. Las políticas corporativas sobre tratamiento de datos de carácter personal, están sujetas a la Ley Orgánica 15/1999 de Protección de Datos de carácter personal (LOPD), así la política de privacidad de la web describe el tratamiento que ésta hace de la información que obtiene de sus clientes. Ello suele reflejarse en determinados apartados a pie de página (parte inferior de la web) con el epígrafe de “Aviso Legal”, “Política de privacidad” o similar.

    - Informarse de las Condiciones Generales de Contratación de la página web. El vendedor debe poner a disposición del consumidor las condiciones generales de compra a las que deba sujetarse el contrato, de manera que puedan ser guardadas e impresas por parte del destinatario, y si necesitas alguna aclaración, no debe dudar en contactar con la empresa.

Medidas técnicas para verificar la seguridad de un sitio web

Se debe comprobar si el sitio posee un certificado de seguridad: un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Es aconsejable observar en la barra de direcciones del navegador y comprobar que la dirección web comienza por “https://”, normalmente es únicamente “http”. De este modo se indica que la información transcurre cifrada y así se evita que un atacante pueda capturar los datos.

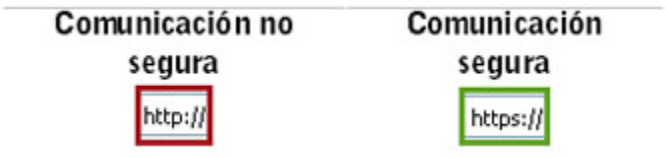


Ilustración 4: Comunicación segura y no segura según el indicativo del protocolo utilizado en la comunicación

También se debe verificar los indicadores de seguridad del sitio web en el cual se ingresará la información personal: cuando una página web tiene un certificado válido, aparece como indicativo un candado en la parte inferior derecha o en la parte superior que indica que se está usando el protocolo de comunicación seguro HTTPS, que garantiza la comunicación segura entre el servidor y el cliente, evitando de ese modo que personas ajenas capturen los datos intercambiados.

En el portal de compra se muestra el candado de maneras distintas dependiendo del tipo de navegador. Al seleccionar con el ratón dicho candado se abre una ventana que contiene todos los datos del certificado SSL, así como los datos de la entidad de certificación que lo generó.

En función del tipo de certificado SSL que se esté utilizando (SSL o EV-SSL), puede aparecer la barra de dirección o parte de la misma de color verde o azul:

Certificados seguros para las páginas web

Certificado SSL-EV (extended-validation)

Es el certificado SSL que incorpora más medidas de seguridad. Es el más seguro y confirma la legitimidad de la página.

El certificado aporta información sobre la empresa a la que se compra, asegurando al usuario que dicha información es cierta.

En los distintos navegadores se vería del siguiente modo:

Ilustración 5: Barra de dirección del navegador Internet Explorer cuando accedemos a una página Web que posee un certificado SSL-EV

Ilustración 6: Barra de dirección del navegador Mozilla Firefox cuando accedemos a una página Web que posee un certificado SSL-EV

Ilustración 7: Barra de dirección del navegador Safari cuando accedemos a una página Web que posee un certificado SSL-EV

Certificado SSL

El certificado SSL que usa la página no proporciona información de identidad, es decir, no se ha llegado a verificar que la dirección pertenece realmente a la entidad.

Por este motivo para poder utilizar la página con unas mínimas garantías el usuario debe estar seguro de que:

- La dirección de la página que va a visitar pertenece a la entidad.
- La dirección en la barra de navegación está bien escrita. En ocasiones los atacantes intentan suplantar las páginas utilizando direcciones similares y creando páginas prácticamente idénticas.

En los distintos navegadores se vería del siguiente modo:

Ilustración 8: Barra de dirección del navegador Internet Explorer cuando accedemos a una página Web que posee un certificado SSL

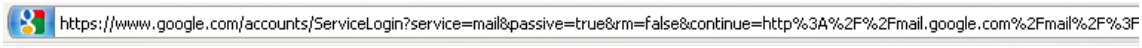


Ilustración 9: Barra de dirección del navegador Mozilla Firefox cuando accedemos a una página Web que posee un certificado SSL

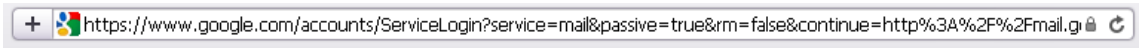


Ilustración 10: Barra de dirección del navegador Safari cuando accedemos a una página Web que posee un certificado SSL

Si es posible, y a fin de asegurar el conocimiento mutuo entre las partes, es aconsejable utilizar la firma electrónica con certificado reconocido (Ley 59/2003 sobre firma electrónica, de 19 de diciembre. En este caso el DNI electrónico incorpora un chip con dicho tipo de firma que facilita la autenticación del usuario.

6.2.4 Comparar y analizar el servicio de la tienda online.

El siguiente paso antes de realizar la compra es comparar y analizar el servicio de la tienda online.

Es recomendable, una vez se tienen todos los datos, comparar el artículo y el servicio de la web de compra en los diferentes portales especializados que permiten valorar el servicio de las tiendas online. Ejemplos de dichos portales son *Ciao* (www.ciao.es), *Dooyoo* (www.doowwyoo.es), *Kelkoo* (www.kelkoo.es) o *Twenga* (www.twenga.es).

También es recomendable acceder a comunidades o foros en la Red que reúnan opiniones imparciales de los consumidores así como información actualizada de los precios y productos ofrecidos por los anunciantes, a la vez que a la web oficial del fabricante donde se puede comprobar que las características técnicas del producto son las mismas que indica el comerciante.

6.2.5 Comprobar las condiciones de compra

La ley 7/1996, de 15 de Enero, de Ordenación del Comercio Minorista en su art. 40 establece que antes de realizar la compra el vendedor deberá informar al consumidor de:

- Las características esenciales del producto.
- El precio total (incluidos los impuestos).
- Los gastos de entrega y transporte.

En particular, y haciendo referencia a las condiciones generales de contratación que se vieron en los pasos anteriores, la idea es definir en concreto éstas en la compra que se pretende realizar. Por ello es recomendable comprobar los datos particulares de la compra y que se disponen referenciados en el listado de arriba.

6.2.6 Confirmación de la compra y acuse de recibo de la misma (fase contractual)

Una vez se han realizado los pasos anteriores de forma correcta, atendiendo a los requisitos de seguridad establecidos, el último paso a la hora de hacer la compra efectiva es aceptar las condiciones de la misma y realizarla.

En ese preciso instante, y según la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, se establece que con posterioridad al acuerdo de compra, el vendedor está obligado a confirmar al comprador que ha recibido su aceptación a la compra del producto o servicio. Esto puede realizarlo de las siguientes maneras:

1) Mediante una página web resumen de la transacción, siempre que permita almacenar o imprimir una copia como comprobante de compra.

   Dicho resumen debe contener cada uno de los conceptos del precio desglosado de forma individual. Así mismo el consumidor ha de tener la opción de modificar dichos datos o anular la compra en el caso de que no le parecieren correctos.

2) Realizando el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el consumidor haya señalado, en el plazo de las 24 horas siguientes a la recepción de la aceptación. Dicho acuse de recibo incluye generalmente un número de pedido que facilita la identificación y resolución de los problemas por parte del servicio postventa.

Este comprobante tiene los mismos efectos legales que un ticket de compra en un comercio tradicional siendo necesario a la hora de ejercer los derechos del consumidor. Por ello es recomendable imprimir y guardar una copia de dicho recibo junto con una copia de los términos y condiciones de la venta así como de las características del producto.

7 SELLOS DE CONFIANZA

A la vez que se instalan y configuran las medidas de seguridad, y se realizan las comprobaciones legales y técnicas sobre la página de compra, también es necesario llevar a cabo unas buenas prácticas para ejecutar una compra/venta segura a través de Internet. En particular, la actuación más importante para ello es verificar la calidad de la empresa que lleva la venta online.

7.1 ¿CÓMO SE VERIFICA SI LA EMPRESA SE ENCUENTRA ADHERIDA A UN SELLO DE CONFIANZA?

La Ley 34/2002 (LSSICE) establece la posibilidad de autorregulación del sector mediante el desarrollo de códigos de conducta voluntarios por parte de corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores.

El Real Decreto 1163/2005 de 30 de septiembre y modificado por la disposición final tercera del Real Decreto 231/2008 de 15 de febrero aprueba el sello de confianza como un logotipo o marca para que los consumidores puedan distinguir aquellos prestadores de servicios que incorporan garantías que proporcionan un elevado nivel de protección de sus derechos.

La información acerca de las características de los sellos de confianza así como las empresas adheridas a los mismos la ofrece la página oficial del Instituto Nacional del Consumo. En la actualidad hay tres códigos de conducta o sellos de confianza que cuentan con el "Distintivo Público de Confianza en Línea" reconocido por el Instituto Nacional del Consumo:

7.1.1 Código de CONFIANZA ON LINE

Promovido por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), Asociación Española de Comercio Electrónico y Marketing Relacional (AECEM) y la entidad pública empresarial Red.es

Código de CONFIANZA ON LINE

7.1.2 Código de CONDUCTA APTICE

Promovido por la Asociación para la promoción de las tecnologías de la Información y el Comercio Electrónico (APTICE).

Asociación para la Promoción de las Tecnologías de la Información y el Comercio Electrónico

Código de CONDUCTA APTICE

7.1.3 Óptima Web: Código de Confianza Online y E-Commerce

Promovido por la Asociación para el fomento del comercio Electrónico Empresarial (ANETCOM)

Óptima Web: Código de Confianza Online y E-Commerce

8 DÓNDE Y COMO RECLAMAR SI LA COMPRA NO ES SATISFACTORIA

Es necesario para el ciudadano conocer los principales métodos de reclamación en el caso de que una compra no haya sido satisfactoria. Las opciones que se presentan para el consumidor son:

- Reclamación ante el servicio postventa de la empresa.
- Reclamación ante la entidad gestora del sello de confianza.
- Reclamación ante las Administraciones de Consumo competentes.
- Resolver las controversias por vía extrajudicial reclamando ante los sistemas arbitrales de consumo.
- Acudir a la vía judicial e interponer demanda ante el tribunal competente.
- Reclamaciones en el extranjero.
- Dónde acudir y denunciar en caso de fraude.

A fin de clarificar dichas vías se exponen a continuación los principales pasos a realizar de cara a la reclamación:

8.1 RECLAMACIÓN ANTE EL SERVICIO POSTVENTA DE LA EMPRESA

Es la primera vía de reclamación de las compras a través de Internet. El servicio postventa de una empresa ha de garantizar la asistencia y soporte al consumidor una vez realizada la compra y ante cualquier problema que pudiera surgir.

A fin de realizar la reclamación correctamente se recomienda incluir los siguientes datos:

1) El número o identificador de factura y la fecha de compra.
2) Su nombre y dirección.
3) Producto adquirido y precio.
4) Objeto de la reclamación.
5) Copias (nunca los originales) de documentos que estén relacionados con la compra (factura, condiciones generales, correos electrónicos intercambiados, etc.)

6) Indicar si prefiere que le cambien el producto por otro o que le devuelvan el dinero.

7) Indicar una fecha máxima en la cual se espera haber recibido una respuesta o acción por parte de la empresa.

A su vez es muy importante guardar una copia de dicha carta, email o fax que se remita y hacer copias de las respuestas recibidas.

8.2 RECLAMACIÓN ANTE LA ENTIDAD GESTORA DEL SELLO DE CONFIANZA

Las compras realizadas en empresas que cuentan con un sello de confianza obligan generalmente a las mismas a aceptar un sistema interno de resolución de conflictos.

Es el caso de empresas adheridas a sellos de calidad como Confianza Online, Calidad Agace y Optima Web, que como se indicó anteriormente cuentan con el distintivo público de confianza en línea.

Dicho sistema es gratuito e imparcial siendo previo a cualquier actuación de la administración.

8.2.1 Cómo reclamar en Confianza Online

Mediante dicho sistema se ofrece un instrumento de resolución extrajudicial de controversias rápido, económico y eficaz. Si se desea reclamar sobre una publicidad interactiva o comercio electrónico se puede hacer desde la siguiente dirección:

http://www.confianzaonline.es/reclamaciones/datos.php

A tal fin cuando una reclamación llega a la secretaría de Confianza Online, para iniciar los trámites correspondientes ésta necesita poder identificar claramente al reclamante, qué se está reclamando (objeto de la reclamación) y contra quién se reclama (empresa reclamada). Por este motivo, es muy importante que el reclamante proporcione, al menos, información detallada sobre los siguientes extremos:

Datos del reclamante

En el caso de que el reclamante sea un consumidor individual, debe aportar una fotocopia del DNI o documento oficial equivalente y los datos de su domicilio, teléfono de contacto, correo electrónico, etc., y, en caso de ser su domicilio diferente al recogido en su documento de identificación, la dirección del mismo.

Si el reclamante es una empresa, debe indicar su denominación o razón social, el domicilio social y, en su caso, los datos personales de su representante legal que, además, deben aportarse al escrito de reclamación.

Datos del reclamado

Éstos deben ser lo más detallados que resulte posible, especialmente en lo relativo al nombre o denominación social del reclamado.

Identificación de la conducta reclamada

El reclamante debe describir de la forma más precisa posible la conducta en cuestión, indicando con claridad los motivos por los que el reclamante considera que se infringe el Código Ético de Comercio Electrónico y Publicidad Interactiva[5]. Los datos relativos a este punto resultan de vital importancia para una correcta tramitación del procedimiento.

Documentación y pruebas

El reclamante debe aportar, junto con su reclamación, todos los documentos y pruebas pertinentes que sirvan de apoyo a sus alegaciones.

Las reclamaciones podrán enviarse de dos formas:

1) Por correo postal a la Secretaría de Confianza Online (Conde de Peñalver, 52 - 3° D - 28006 Madrid) o por fax al número: 91 402 83 39 de acuerdo con el siguiente formulario:

2) Rellenando y enviando el siguiente formulario online:

En ambos casos, una vez recibida la reclamación, la Secretaría de Confianza Online se pondrá en contacto con el interesado.

8.3 RECLAMACIÓN ANTE LAS ADMINISTRACIONES DE CONSUMO COMPETENTES

Si la respuesta obtenida no es satisfactoria, se pueden interponer reclamaciones ante la administración competente en materia de consumo. A tal fin es recomendable acudir a la Oficina Municipal de Información al Consumidor[6] (OMIC) de su localidad.

La función de dichas oficinas es informar y orientar a los consumidores en el ejercicio de sus derechos, a la vez que remiten las reclamaciones y denuncias presentadas a los organismos competentes en razón de la materia o territorio para su resolución.

La Administración competente una vez recibida la denuncia inicia una mediación con la empresa con la que el consumidor mantiene la disputa a fin de llegar a un acuerdo entre ambas partes.

En dichas oficinas se le facilita al usuario a su vez un modelo de formulario de cara a presentar la reclamación. Si bien dicha formalidad no es obligatoria.

[5] Disponible en: http://www.autocontrol.es/pdfs/Cod_ConfianzaOnline.pdf

[6] Se pueden consultar las direcciones de estas administraciones en: http://consumo-inc.es/directorio/interior/omic/omic.htm

A fin de presentar la denuncia será necesario incluir:

- La identificación de la empresa reclamada.
- El objeto de la queja.

Una vez recibida la denuncia o reclamación el órgano competente inicia las acciones pertinentes para la determinación y comprobación de las mismas abriendo en su caso el procedimiento sancionador.

8.4 RECLAMACIÓN ANTE LOS SISTEMAS ARBITRALES DE CONSUMO

El arbitraje electrónico de consumo tiene las siguientes características:

- Gratuidad
- Accesibilidad
- Especialización
- Agilidad
- Voluntariedad

El art 23 de la LSSICE establece que es necesario que conste la voluntad inequívoca de las partes de someter el litigio a los árbitros y la de cumplir el laudo emitido por los mismo.

La solicitud de arbitraje ha de formalizarse personalmente ante la Junta Arbitral de Consumo a la que ambas partes, de común acuerdo, sometan la resolución del conflicto, o en su defecto la que corresponda al domicilio del consumidor.

El caso es resuelto por un tribunal integrado por tres árbitros que garantiza una solución imparcial y objetiva, siendo la resolución dictada por el tribunal vinculante, de obligado cumplimiento para las partes y cerrando el acceso a la vía judicial.

El arbitraje de consumo podrá realizarse a su vez de forma telemática a través de Internet, en aquellas Juntas Arbitrales que voluntariamente se hayan adscrito a la administración de arbitraje electrónico. Este se realiza íntegramente a través de sistemas electrónicos, desde la solicitud, hasta la terminación del procedimiento, incluyendo las notificaciones.

Para que la reclamación del consumidor pueda realizarse mediante el Sistema Arbitral de Consumo, la empresa debe haberse adherido al mismo, lo que puede comprobarse desde la Oficina virtual de dicho sistema en la siguiente dirección:

http://arbitrajedeconsumo.msc.es

8.5 SISTEMA JUDICIAL

La última opción que se les presenta a los consumidores, es acudir a la vía judicial reclamando ante los Tribunales Ordinarios de Justicia las indemnizaciones por daños y perjuicios.

Cabe emprender dos vías, la vía civil y la vía penal (si entiende que la actuación de la tienda online pueda entrever la comisión de un delito).

Si bien a la hora de realizar una reclamación judicial es necesario sopesar el coste tanto de la consulta jurídica así como de los costes judiciales en relación al valor de lo que se quiere reclamar, dado que el coste del procedimiento puede exceder en numerosas ocasiones el valor de lo reclamado.

8.6 RECLAMACIONES EN EL EXTRANJERO

El Reglamento Comunitario 44/2001 estable que el consumidor puede:

- Demandar ante los tribunales del Estado miembro en el que estuviere domiciliado el empresario
- Demandar ante los tribunales del Estado donde estuviere domiciliado el consumidor (Forum Actoris)

En base a la normativa internacional y comunitaria sobre la materia (Convenio de Roma de 1980 y Reglamento Roma I), el consumidor estará protegido, dado que:

- El juez aplicará la ley elegida por las partes en su contrato, siempre que esta elección no prive al consumidor de la protección de las disposiciones imperativas de la ley del país en que tenga su residencia habitual.
- En ausencia de elección, los contratos de consumo se regirán por la ley del país en que el consumidor tenga su residencia habitual (Art. 5.3 CR)

8.7 EN CASO DE FRAUDE

La colaboración de los clientes y usuarios del servicio afectado es fundamental para poder interceptar a tiempo los intentos de fraude y poder localizar lugares desde donde se publican páginas, se emiten mensajes fraudulentos o donde se reciben los datos capturados.

Para facilitar esta colaboración, la Oficina Seguridad del Internauta pone a su disposición un formulario de alta de incidentes, desde donde el usuario puede indicarle las entidades afectadas y la información disponible sobre el caso de fraude, así como el teléfono de asistencia 901 111 121.

Si se ha sido víctima de un fraude, es conveniente poner inmediatamente la denuncia correspondiente. A tal efecto puede ponerse en contacto con:

8.7.1 Dirección General de la Policía (www.policia.es)

La Dirección General de la Policía, a través de la Comisaría General de Policía Judicial, ha creado la Brigada de Investigación Tecnológica operativa las 24 horas, para combatir la delincuencia que utiliza los medios que proporcionan las nuevas Tecnologías de la Información.

Las denuncias pueden realizarse en el teléfono: 91.582.29.00, ó por correo electrónico: delitos.tecnologicos@policia.es.

La presentación de la denuncia se puede realizar a través del teléfono: 902 102 112, en el portal de la policía o en cualquier comisaría.

8.7.2 Dirección General de la Guardia Civil (www.guardiacivil.es)

La Dirección General de la Guardia Civil cuenta con el Grupo de Delitos Telemáticos (GDT) de la Unidad Central Operativa (UCO), con el que se puede contactar a través de la sección colabora de su página web o del correo electrónico: delitostelematicos@guardiacivil.org

8.7.3 Policías autonómicas

Las policías autonómicas también tienen sus propios grupos especializados en delitos relacionados con las nuevas tecnologías:

La Ertzaintza dispone de la Sección Central de Delitos en Tecnologías de la Información con la que se puede contactar a través del correo: delitosinformaticos@ertzaintza.net

Los Mossos d'Esquadra trabajan de forma especializada desde la Unidad de Central de Delitos Informáticos con la que se puede conectar a través de las formas de contacto que se indican en su página web.

Instituto Nacional
de Tecnologías
de la Comunicación