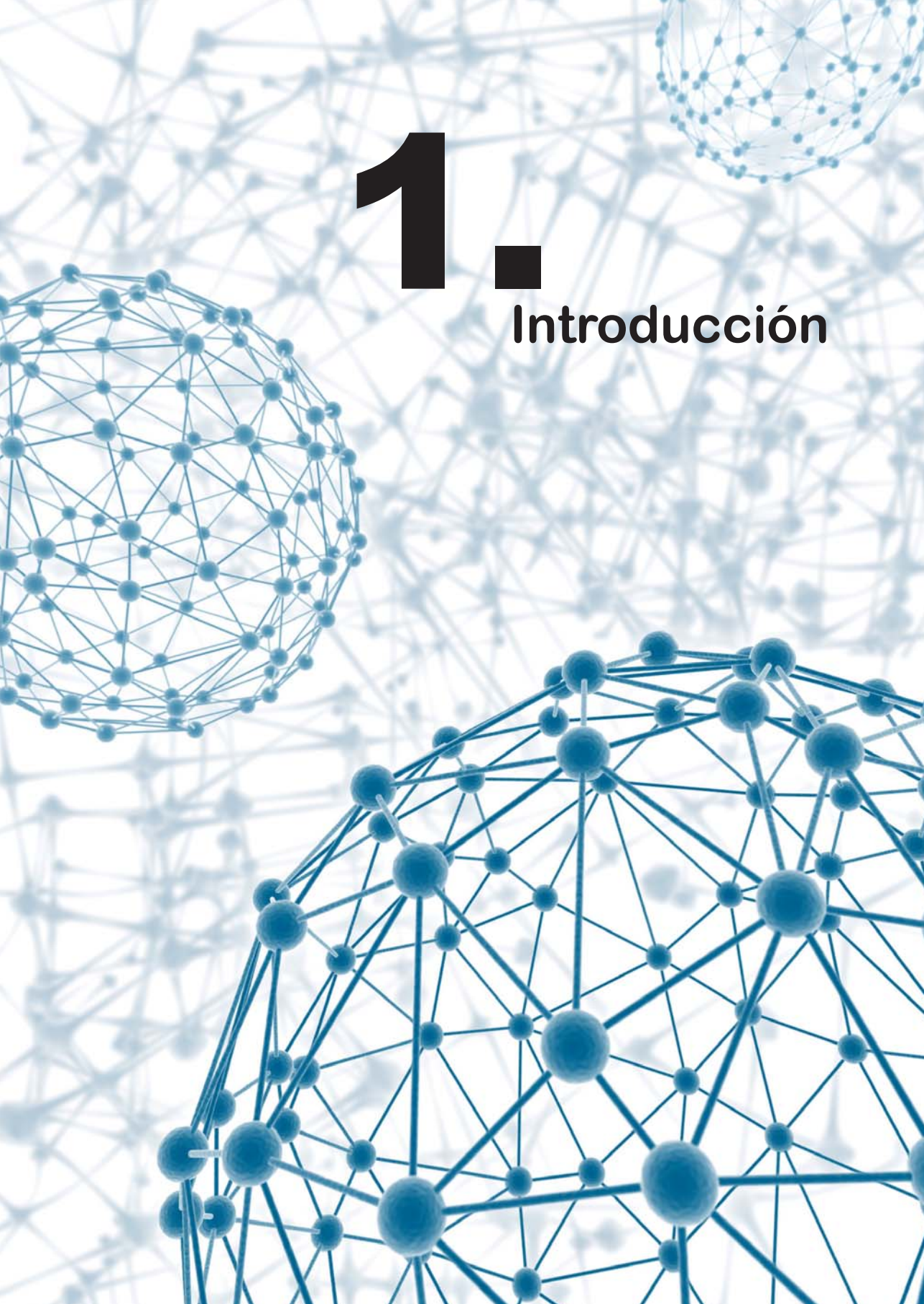
El SPAM

qué es y cómo enfrentarte a él

facua

Consumidores en Acción



1. Introducción

1 INTRODUCCIÓN

Con el paso del tiempo y especialmente en los últimos años, se ha asistido a un avance en la sociedad de la información que está transformando los mecanismos tradicionales de intercambio de información, especialmente en lo que se refiere al tiempo y la distancia, ya que los contenidos pueden dirigirse fácilmente y de una forma asequible a una audiencia masiva y de una forma muy rápida.

Este hecho no ha pasado desapercibido para las empresas, que han comenzado a usar Internet como un nuevo canal de ventas, como una alternativa más a la forma tradicional.

Sin embargo, con el paso del tiempo, este cambio también ha ido aparejado la introducción de nuevos métodos de publicidad masiva que ha invadido a los consumidores de correos electrónicos no autorizados y de llamadas promocionales no solicitadas que están causando unas molestias considerables a los consumidores.

2. Definición de *spam*

2 DEFINICIÓN DE *SPAM*

El *spam* se define como los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva a muchos usuarios al mismo tiempo. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono.

El término *spam* proviene de la contracción de *Spiced Ham* (carne especiada), un producto muy comercializado en Reino Unido durante la Segunda Guerra Mundial. Años más tarde, el grupo humorístico británico The Monty Python fue el responsable de otorgarle el significado que tiene hoy *spam* tras popularizar una broma televisiva en la que sus protagonistas repetían esta palabra en innumerables ocasiones, de la misma manera en que ahora lo hace el correo no deseado.

El spam es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del total del tráfico de correo electrónico.

El primer caso de *spam* pudo comenzar en 1978, con una carta enviada por la empresa Digital Equipment Corporation. Esta compañía remitió un anuncio sobre su ordenador DEC-20 a todos los usuarios de ArpaNet (precursora de Internet) de la costa occidental de los Estados Unidos.

Posteriormente apareció en Usenet un anuncio de un despacho de abogados que informaba de un servicio propio para rellenar formularios que daba acceso a un permiso para trabajar en Estados Unidos. Este anuncio fue enviado mediante un script a los grupos de discusión que existían por aquel entonces.

Desde ese momento su uso se fue desarrollando hasta llegar a la situación actual en la que se ha desarrollado especialmente a través del uso del correo electrónico de forma masiva.

Este tipo de mensajes de correo electrónico presentan una serie de características:

- Suelen tener un contenido publicitario: métodos para obtener dinero fácilmente, productos milagro, supuestas ofertas inmobiliarias o catálogos de productos en venta en promoción a un precio especialmente bajo.
- Suelen presentar un asunto llamativo que intenta captar la atención de las personas a las que va dirigida.
- La mayoría del *spam* tiene su origen en Estados Unidos o Asia. No obstante, cada vez es más común el *spam* en español. Por ello, y al tratarse en muchas ocasiones de traducciones de poca calidad, la redacción del escrito suele presentar imperfecciones semánticas y faltas de ortografía.
- La dirección que aparece como remitente del mensaje no resulta conocida para el usuario, siendo habitual también en ocasiones que esté falseada.
- El mensaje no suele tener la posibilidad de contestarlo.

Anteriormente se ha señalado que el método de distribución más habitual es el correo electrónico. No obstante, existen diferentes variantes, cada cual con su propio nombre, asociado en función del canal de distribución:

- *Spam* en sentido estricto: enviado a través del correo electrónico.
- *Spam* SMS: *spam* destinado a enviarse a dispositivos móviles mediante SMS (Short Message Service).
- *Spim:* específico para aplicaciones de tipo mensajería instantánea (MSN Messenger, Yahoo Messenger, etc).

- *Spit: spam* sobre telefonía IP que consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.

El *spam* es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del total del tráfico de correo electrónico. Además, a medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el *spam*, los *spammers* (usuarios maliciosos que se dedican profesionalmente a enviar *spam*) se vuelven a su vez más sofisticados, y modifican sus técnicas con objeto de evitar las contramedidas desplegadas por los usuarios.

Las personas que envían *spam* tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios. Con este objeto, utilizan distintas técnicas, algunas de ellas altamente sofisticadas:

- Listas de correo: el *spammer* se da de alta en la lista de correo, y anota las direcciones del resto de miembros.
- Uso de programas automáticos que recorren Internet en busca de direcciones en páginas web, grupos de noticias, weblogs, etc.
- Compra de bases de datos de usuarios a particulares o empresas: este tipo de actividad incumple directamente lo establecido en la Ley Orgánica

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo.

- Técnicas a través de las cuáles el *spammer* genera direcciones de correo electrónico pertenecientes a un dominio específico, y envía mensajes a las mismas. El servidor de correo del dominio responderá con un error a las direcciones que no existan realmente, de modo que el *spammer* puede averiguar cuáles de las direcciones que ha generado son válidas. Las direcciones pueden componerse mediante un diccionario o mediante fuerza bruta, es decir, probando todas las combinaciones posibles de caracteres.

Por lo tanto, todos los usuarios del correo electrónico corren el riesgo de ser víctimas de estos intentos de ataques. Asimismo, cualquier dirección pública en Internet (que haya sido utilizada en foros, grupos de noticias o en algún sitio web) será más susceptible de ser víctima del *spam*.

Actualmente hay empresas que facturan millones de dólares al año recolectando direcciones de correo electrónico, vendiéndolas y enviándole mensajes de promociones, ofertas, y publicidad no solicitada.

Las personas que envían *spam* tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas.

3.

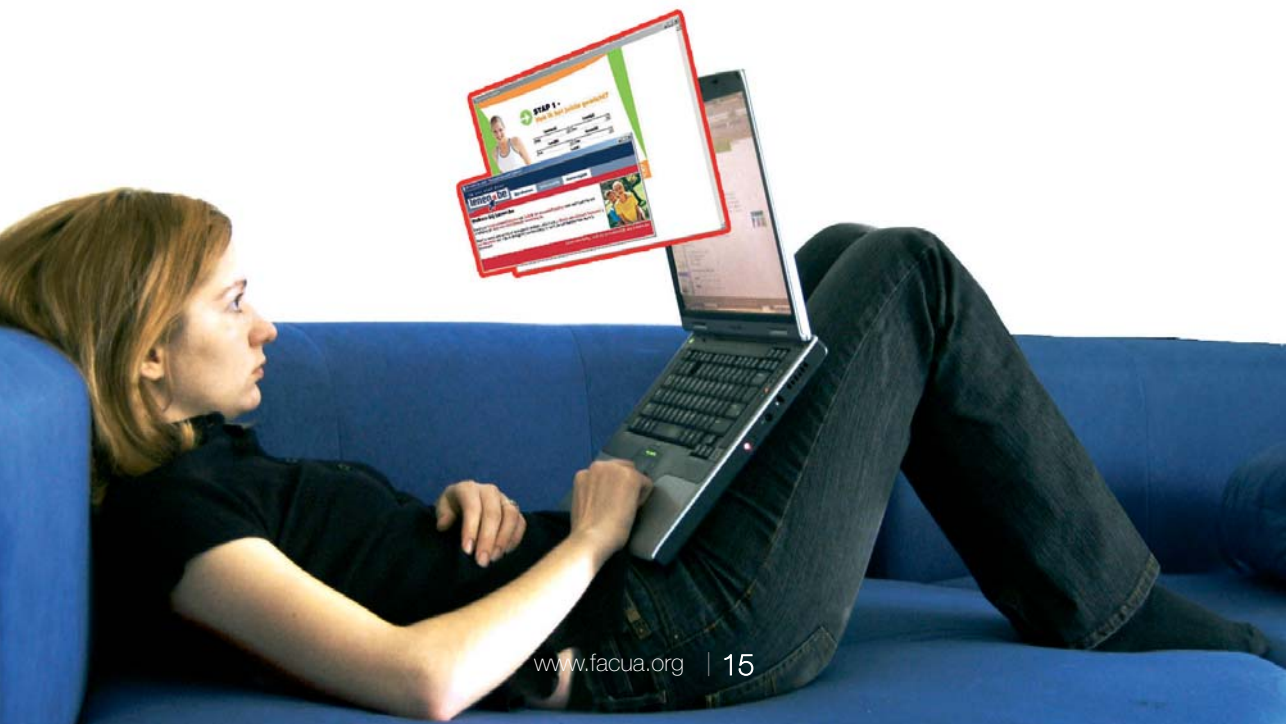
Algunas técnicas específicas de *spam*

3 ALGUNAS TÉCNICAS ESPECÍFICAS DE *SPAM*

Junto a lo que se conoce de forma genérica como *spam*, con el paso del tiempo se han ido desarrollando técnicas más desarrolladas que por los métodos característicos que siguen y por el importante número de consumidores a los que puede llegar han adoptado nombres específicos.

Spam por ventanas emergentes (Pop ups)

Es el efecto que se produce cuando al estar conectado a Internet emerge un mensaje no solicitado. Generalmente se trata de un mensaje de carácter publicitario.

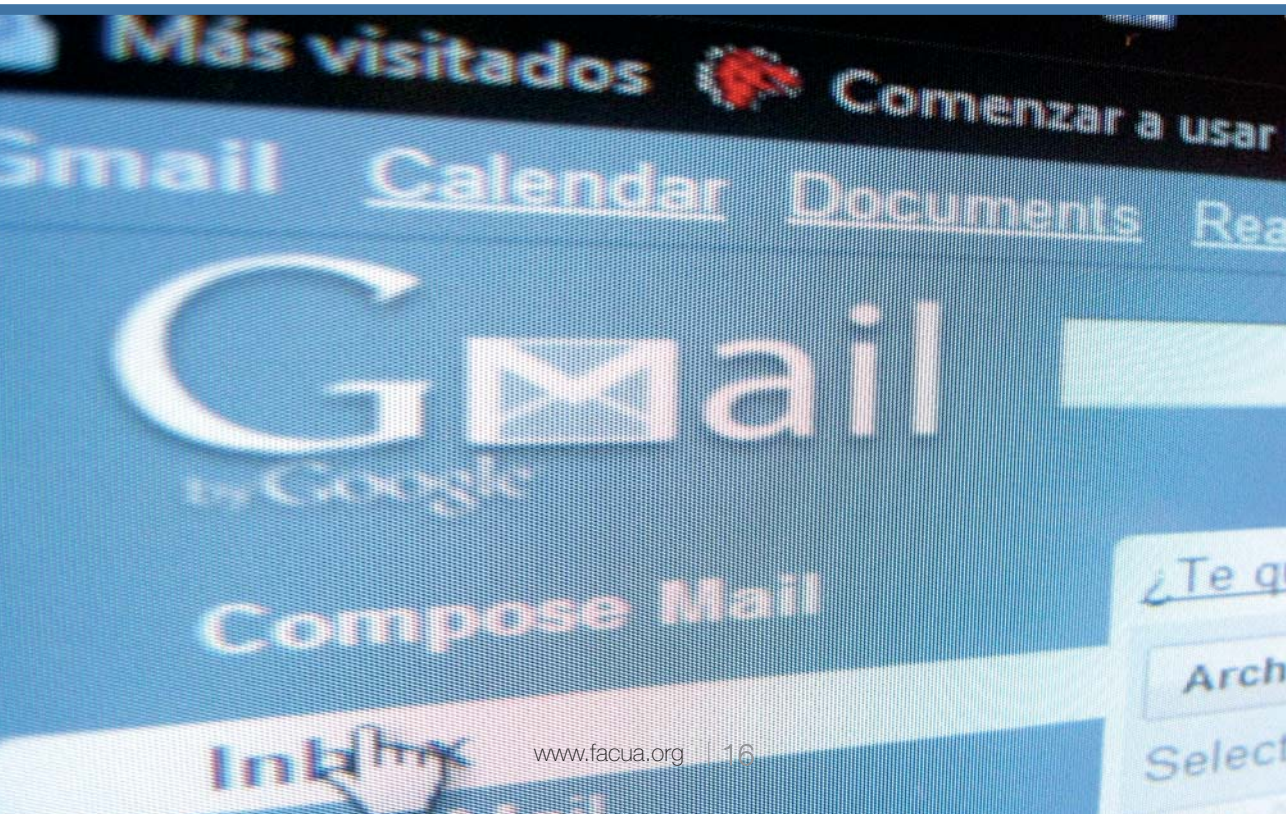


Para ello se utiliza una funcionalidad del sistema de explotación Windows, disponible sobre las versiones Windows NT4, 2000, XP o Windows 7 y que permite a un administrador de redes enviar mensajes a otros puestos de la red.

La solución más sencilla para evitar estas ventanas emergentes consiste en desactivar este servicio de Windows. Otro método consiste en utilizar un corta-fuegos destinado a filtrar los puertos TCP y UDP (135, 137,138, 139 y 445) del ordenador, pero con esta medida es posible que deje de funcionar la red.

Hoax

El *hoax* es un mensaje de correo electrónico, normalmente distribuido en cadena, que tiene un contenido falso o engañoso.



Algunos *hoax* informan sobre la existencia de supuestos virus o contienen fórmulas para ganar millones, o crean cadenas de la suerte. También los hay que contienen mensajes de solidaridad.

Los *hoax*, normalmente, pretenden captar direcciones de correo o saturar la red o los servidores de correo.

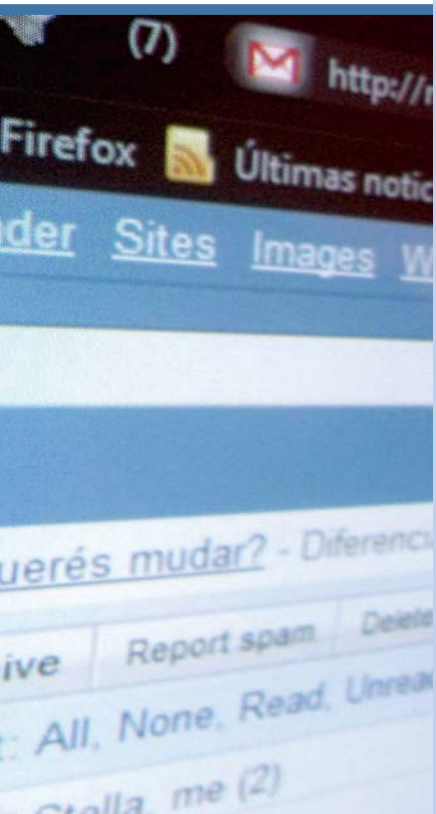
Phishing

El *phishing* es la capacidad de duplicar una web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos, duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

En ocasiones, el término *phishing* se dice que es la contracción de *password harvesting fishing* (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo.

De forma más general, el nombre de *phishing* también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un correo-e parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación.

El término *phishing* fue creado a mediados de los años 90 por los *crackers* que procuraban robar las cuentas de America *online* (AOL). Un atacante se presentaría como empleado de AOL y enviaría un mensaje inmediato a una víctima potencial. El mensaje pediría que la víctima revelara su contraseña, con variadas excusas como la verificación de la cuenta o confirmación de la información de la facturación.



Una vez que la víctima entregara la contraseña, el atacante podría tener acceso a la cuenta de la víctima y utilizarla para cualquier otro propósito, tales como el envío de publicidad no solicitada (*spamming*).

En los últimos años, han trascendido intentos de estafas a clientes de distintas entidades bancarias mediante lo que se denomina *phishing*.

FACUA ha alertado en diferentes ocasiones de este nuevo caso de *phishing* o estafa bancaria por Internet a clientes de distintas entidades bancarias mediante el envío masivo e indiscriminado de un correo electrónico mediante el que se intentan recabar los datos de los usuarios para acceder a sus cuentas bancarias.

El phishing es la capacidad de duplicar una web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada.

En el correo-e aparece como remitente el nombre de la entidad bancaria, con la supuesta dirección de su correo electrónico y especificando el asunto, relacionando con un proceso de notificación. Suele aparecer además una imagen que reproduce el logotipo de la entidad bancaria, y a veces se acompaña de un mensaje que invita a entrar en la página web del banco.

En algunos de los fraudes detectados, el texto del correo-e advertía al usuario que la entidad bancaria ha renovado su sistema de seguridad para prevenir las tentativas de estafa, lo que hace necesario, indica, que reactive su cuenta a causa de las correcciones del programa de seguridad.

FACUA advierte a los usuarios que las entidades bancarias no verifican sus datos confidenciales mediante mensajes de correo electrónico, por lo que deben desconfiar de los que reciban aunque reproduzcan a la perfección los logotipos y el resto de señas de identidad de dichas empresas.

Asimismo, FACUA reivindica a la banca que debe mejorar los protocolos de seguridad de sus páginas web para evitar que este tipo de estafas puedan tener éxito. Igualmente se pone de manifiesto la necesidad

de que el sector bancario español ponga en marcha campañas de comunicación dirigidas a los usuarios para darles a conocer estas prácticas fraudulentas.

Consejos para evitar el *phishing*

En muchas ocasiones, las empresas dedicadas a enviar *phishing*, utilizan métodos que son cada vez más sofisticados y cuya última intención es conseguir que el usuario de correo electrónico termine revelando sus claves bancarias o números secretos de acceso a cuentas financieras. Algunas de las recomendaciones para no caer en el *phishing* son:

- No atender correos electrónico escritos en idiomas que no conozcas: la entidad financiera no se dirigirá al usuario en ese idioma si antes no lo ha pactado previamente.
- No atender correos enviados por entidades de las que el usuario no sea cliente en los que se pidan datos íntimos o que afecten a tu seguridad.
- No atender sorteos u ofertas económicas de forma inmediata e impulsiva.
- No atender correos que te avisen del cese de actividades financieras recibidos por primera vez y de forma sorpresiva.
- No atender correos de los que se sospeche sin confirmarlos telefónica o personalmente con la entidad firmante.

Además, el Centro de Alerta Antivirus cuenta con una página dedicada más ampliamente al Fraude Financiero a través de Internet.

Para evitar caer en páginas trampa, es recomendable teclear la dirección del banco *online* o tenerla guardada en *Favoritos*. En cualquier caso, hay que


Enter your log in number
OK

evitar acceder a la web de la entidad financiera a través de mensajes de correo electrónico o páginas web de terceros.

Una de las formas de identificar una página web segura, que debe ser empleada por los servicios de banca *online*, es cerciorarse de que la dirección comienza por https, en lugar de http.

Pharming

Al aumento de los intentos de ataques por *phishing* hay que sumar la aparición de nuevas formas de estafas *online*. Una de ellas, conocida como pharming, se perfila como una posible amenaza mucho más sofisticada que el *phishing*.

Consiste en alterar las direcciones DNS que utilizan los usuarios para poder navegar por Internet. Así, por ejemplo, en caso de teclear la dirección de su servicio de banca electrónica, llegan hasta una página web que imita la original a la perfección, pero que, en realidad, ha sido confeccionada por un pirata informático que es quien recibe los datos que los usuarios introducen en ella.

Básicamente, consiste en la manipulación de la resolución de nombres en Internet, llevada a cabo por algún código malicioso que se ha introducido en el equipo. Así cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica.

Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS (Domain Name Server). En ellos se almacenan tablas con las direcciones IP de cada nombre de dominio.

A una escala menor, en cada ordenador conectado a Internet hay un fichero en el que se almacena una

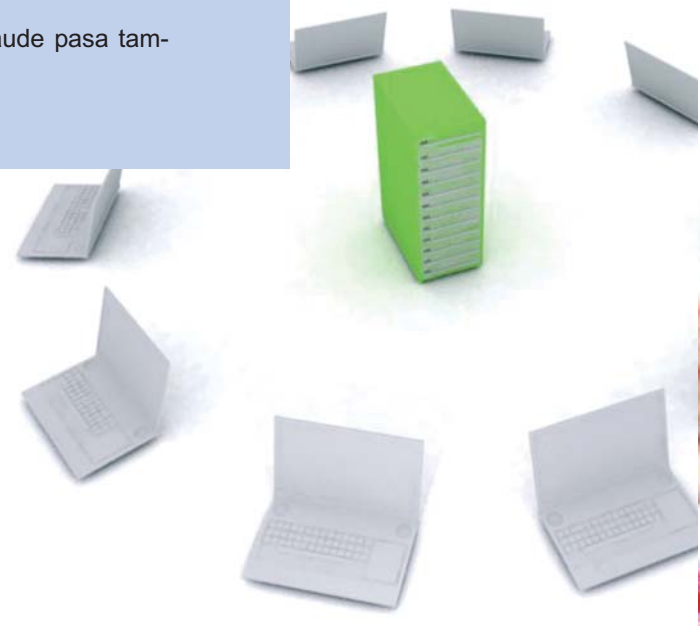
pequeña tabla con nombres de servidores y direcciones IP, de manera que no haga falta acceder a los DNS para determinados nombres de servidor, o incluso para evitarlo.

El *pharming* consiste por tanto en modificar este sistema de resolución de nombres, de manera que cuando el usuario crea que está accediendo a su banco en Internet, realmente está accediendo a la IP de una página web falsa.

El *phishing* debe su éxito a la ingeniería social, aunque no todos los usuarios caen en estos trucos y su éxito está limitado. Y además, cada intento de *phishing* se debe dirigir a un único tipo de servicio bancario, por lo que las posibilidades de éxito son muy limitadas. Por el contrario, el *pharming* puede atacar a un número de usuarios muchísimo mayor.

Además, el *pharming* no se lleva a cabo en un momento concreto, como lo hace el *phishing* mediante sus envíos, ya que la modificación de DNS queda en un ordenador, a la espera de que el usuario acceda a su servicio bancario. De esta manera, el atacante no debe estar pendiente de un ataque puntual, como hemos mencionado antes.

El remedio para esta técnica de fraude pasa también por las soluciones de seguridad.



4.

Regulación legislativa sobre el envío o comunicación de publicidad no deseada (*spam*)

4 REGULACIÓN LEGISLATIVA SOBRE EL ENVÍO O COMUNICACIÓN DE PUBLICIDAD NO DESEADA (*SPAM*)

Introducción

En primer lugar, habría que poner de manifiesto que cuando se habla de envío o comunicación de publicidad no deseada, en el ordenamiento jurídico aparecen reguladas tres formas de canalizar las mismas asociadas al término práctica conocida como *spam*.

- **A través de llamadas telefónicas.**
- **A través de mensajes cortos SMS.**
- **A través de correo electrónico.**

Normativa genérica

De forma genérica, la Directiva 2005/29/CE, del Parlamento Europeo y del Consejo, relativa a las prácticas comerciales desleales de las empresas en su relaciones con los consumidores en el mercado interior, que modifica la Directiva 54/450 CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE, del Parlamento Europeo y del Consejo y el Reglamento(CE) nº 2006/2004 del Parlamento Europeo y del Consejo ("Directiva sobre las prácticas desleales"), establece en su considerando 16º lo siguiente:

"Las disposiciones sobre las prácticas comerciales agresivas deben abarcar aquellas prácticas que mermen de forma significativa la libertad de elección

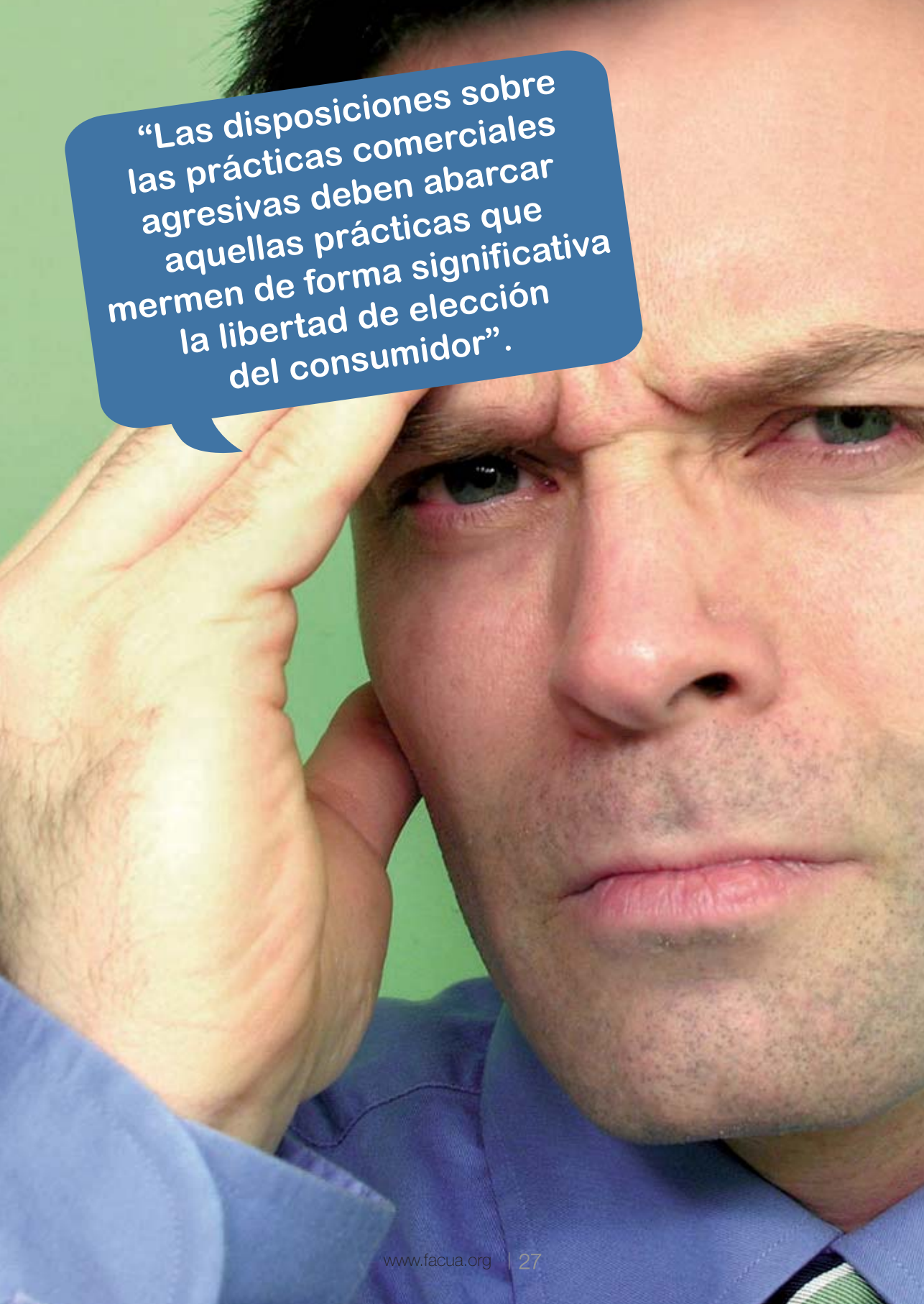
del consumidor. Se trata de las prácticas que utilizan el acoso, la coacción, incluido el uso de la fuerza física, y la influencia indebida".

Ya dentro del articulado, dentro de la Sección Segunda (*"Prácticas Comerciales agresivas"*) los artículos 8º y 9º desarrollan de forma más específica qué es lo que se entiende como prácticas comerciales agresivas, considerando como tales *"toda práctica comercial que, en su contexto fáctico, teniendo en cuenta todas sus características y circunstancias, merme o pueda mermar de forma importante, mediante el acoso, la coacción, incluido el uso de la fuerza, o la influencia indebida, la libertad de elección o conducta del consumidor medio con respecto al producto y, por consiguiente, le haga o pueda hacerle tomar una decisión sobre una transacción que de otra forma no hubiera tomado".*

Asimismo se establece que para determinar si una práctica comercial hace uso del acoso, la coacción, con inclusión del uso de la fuerza, o la influencia indebida se tiene que tener en cuenta el momento y el lugar en que se produce, su naturaleza o su persistencia.

Dicha Directiva se tradujo posteriormente en la aprobación de la Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de los consumidores y usuarios, por medio de la cual en su artículo primero se modificaba la Ley 3/1991, de 10 de enero, de Competencia Desleal, cuyos artículos 19º y 29º hacen referencia de forma específica al problema del *spam*.

Tras dicha modificación, se definió cuáles eran las prácticas comerciales que debían entenderse como desleales con los consumidores, estableciendo de forma específica que *se considera desleal por agresivo realizar visitas en persona al domicilio del consumidor o usuario, ignorando sus peticiones para que el*


“Las disposiciones sobre las prácticas comerciales agresivas deben abarcar aquellas prácticas que mermen de forma significativa la libertad de elección del consumidor”.

empresario o profesional abandone su casa o no vuelva a personarse en ella… Igualmente se reputa desleal realizar propuestas no deseadas y reiteradas por teléfono, fax, correo electrónico u otros medios de comunicación a distancia, salvo en las circunstancias y en la medida en que esté justificado legalmente para hacer cumplir una obligación contractual.

En este sentido, también se establece que el empresario o profesional deberá utilizar en estas comunicaciones sistemas que le permitan al consumidor dejar constancia de su oposición a seguir recibiendo propuestas comerciales de dicho empresario o profesional. Para que el consumidor o usuario pueda ejercer su derecho a manifestar su oposición a recibir propuestas comerciales no deseadas, cuando éstas se realicen por vía telefónica, las llamadas deberán realizarse desde un número de teléfono identificable.

Además, todo ello debe entenderse sin perjuicio de lo establecido en la normativa vigente sobre protección de datos personales, servicios de la sociedad de la información, telecomunicaciones y contratación a distancia con los consumidores o usuarios, incluida la contratación a distancia de servicios financieros".

Algunos operadores de telecomunicaciones (Telefónica, Vodafone, France Telecom-Orange, Yoigo y Ono) pactaron en su día un código ético interno, que incorporaba una veintena de puntos, que, al tratarse de una autorregulación no supone sanción alguna en caso de incumplimiento.

Regulación específica del servicio de voz (llamadas)

En lo que se refiere a la regulación específica de las llamadas no deseadas, el artículo 69º del Real Decreto 424/2005, de 15 de abril por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, establece en su artículo 69º que *"las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas de llamada automática, a través de servicios de comunicaciones electrónicas, sin intervención humana (aparatos de llamada*

automática) o facsímil (fax), sólo podrán realizarse a aquellos que hayan dado su consentimiento previo, expreso e informado.

Además establece que el incumplimiento de dicha norma será sancionado de acuerdo con lo establecido en el artículo 38.3.c, o en el artículo 38.4.d de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Por otra parte, las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas distintos de los arriba mencionados podrán efectuarse salvo las dirigidas a aquellos que hayan manifestado su deseo de no recibir dichas llamadas. Sin embargo, para realizar las llamadas a las que éste se refiere a quienes hubiesen decidido no figurar en las guías de comunicaciones electrónicas disponibles al público o a los que hubiesen ejercido su derecho a que los datos que aparecen en ellas no sean utilizados con fines de publicidad o prospección comercial, será preciso contar con el consentimiento expreso de los mismos".

Con independencia de todo lo señalado anteriormente, cabe señalar que algunos operadores de telecomunicaciones (Telefónica, Vodafone, France Telecom-Orange, Yoigo y Ono) pactaron en su día un código ético interno, que incorporaba una veintena de puntos, que, al tratarse de una autorregulación no supone sanción alguna en caso de incumplimiento.

Regulación específica de los mensajes SMS y correo electrónico

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercial electrónico, establece en su artículo 21º que queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación

electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Sin embargo, continúa diciendo, *"que ello no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.*

No obstante, el prestador deberá ofrecer en todo caso al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija".

Por otra parte, el artículo 38.3 estipula como infracción grave *"el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21".*

Regulación sobre los derechos de acceso y cancelación de los datos de carácter personal

El artículo 15º de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece que el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el

origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicho derecho de acceso sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes

La cancelación de la información personal de los usuarios que aparezca en bases de datos está regulada en la Ley Orgánica de protección de datos de carácter personal.

Por otra parte, el artículo 16º de dicha normativa añade que el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. Con independencia de lo anterior tendrán que ser rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Asimismo, si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

Los datos de carácter personal tendrán que ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones

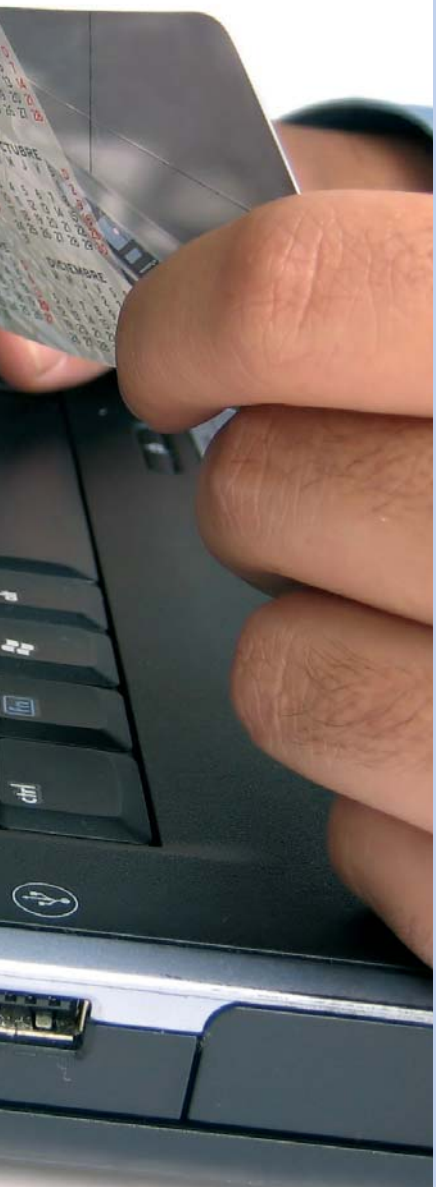
contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación están establecidos reglamentariamente en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Concretamente en su Título III.

En dicho Título cabe destacar lo establecido en los artículos 24º y 25º, los cuáles establecen que los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro. Asimismo, se estipula que el interesado debe disponer de un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan. En este sentido, no se considerarán conforme a la normativa los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

Asimismo, se establece que cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá



concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

Por último, se estipula que el responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud que la comunicación haya sido dirigida al responsable del fichero y que ésta contenga los siguientes elementos:

- Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente. Todo ello sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

  - Petición en que se concreta la solicitud.

  - Dirección a efectos de notificaciones, fecha y firma del solicitante.

  - Documentos acreditativos de la petición que formula, en su caso.

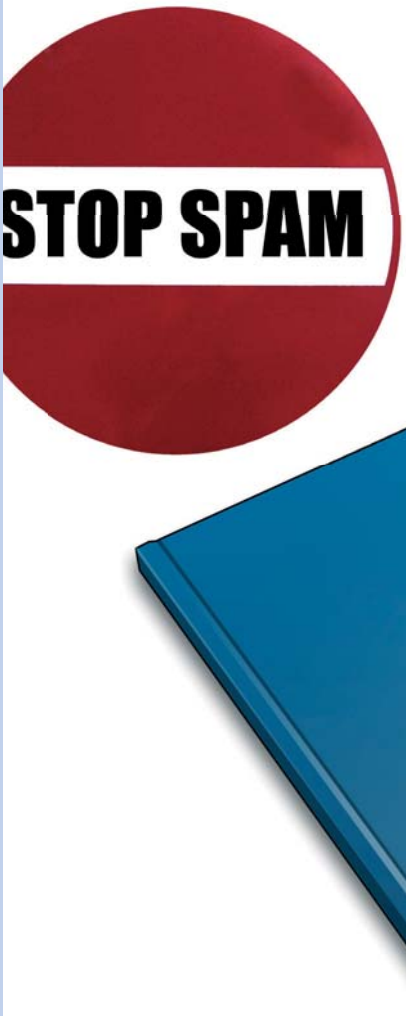
Regulación sobre los ficheros comunes de exclusión del envío de comunicaciones comerciales

El artículo 49º del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, estipula que es posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad, debiendo contener los citados ficheros los mínimos datos imprescindibles para identificar al afectado.

Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento. El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

Por último, se establece que quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que



pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Recomendaciones para evitar y reducir el *spam*

Recomendaciones para prevenir la recepción de *spam:*

- No enviar ni participar en mensajes en cadena, ya que los mismos generalmente son algún tipo de engaño cuyo objetivo es captar el mayor número de direcciones posibles.
- Si deseas enviar mensajes a muchos destinatarios, hazlo siempre con copia oculta (CCC), ya que esto evita que un destinatario vea y pueda hacerse con el correo electrónico de los demás destinatarios.
- No publicar una dirección privada en sitios webs, foros, conversaciones *online*, etc. ya que sólo facilita la obtención de las mismas a los *spammers* (personas que envían *spam*). En el caso de que fuera necesario publicar la dirección de correo electrónico en alguna web, es recomendable, siempre que el programa lo permita, que se utilicen las expresiones *"at"* o *"arroba"* en vez de *"@"*, para evitar que los programas creadores de *spam* puedan capturar y hacerse con la dirección de correo electrónico.
- Si se desea navegar o registrarse en sitios de baja confianza, hay que hacerlo con cuentas de *mails* destinadas para ese fin. Algunos servicios de *webmail* disponen de esta funcionalidad: protegen la dirección de correo electrónico, mientras se puede publicar otra cuenta y administrar ambas desde el mismo lugar.

- Para el mismo fin, también es recomendable utilizar cuentas de correo temporales y descartables para proporcionarlas en aquellos casos en los que no se conozca o no se confíe en la persona destinataria, dejando una dirección personal para uso exclusivamente personal (familiares, amigos) y otra de carácter laboral o profesional, la cual sólo se debe facilitar a aquellas personas u organizaciones que se conozcan o en la que se tenga suficiente confianza.

- Elegir una dirección de correo electrónico que sea difícil de descubrir o de generar por los programas informáticos, ya que los *spammer* cuentan con este tipo de programas que generan automáticamente posibles direcciones de correo electrónicos utilizando combinaciones con listas de palabras que suelen contener campos como alias, apellidos, meses del año o días se la semana, nombre de lugares o de ciudades, signos del zodíaco, etc.

- No responder nunca a este tipo de mensajes ni pinchar sobre los anuncios de correo basura, ya que con esto sólo se confirma la dirección de correo electrónico y sólo se logra recibir más correo basura.

Por ello, es conveniente desactivar la opción de envío de acuse de recibo automático, ya que si un *spammer* recibe dicho acuse sabrá que la dirección se encuentra activa. En este sentido, y al proceder la mayoría de dichos mensajes del extranjero, no tienen incorporado el procedimiento sencillo y gratuito para que los destinatarios puedan solicitar no recibir más mensajes.

- Leer detenidamente las Políticas de Privacidad de las empresas antes de proporcionar cualquier tipo de dato de carácter personal como la dirección de correo electrónico, ya que en muchas ocasiones se ceden los datos de forma inconsciente a las filiales de estas empresas o bien se

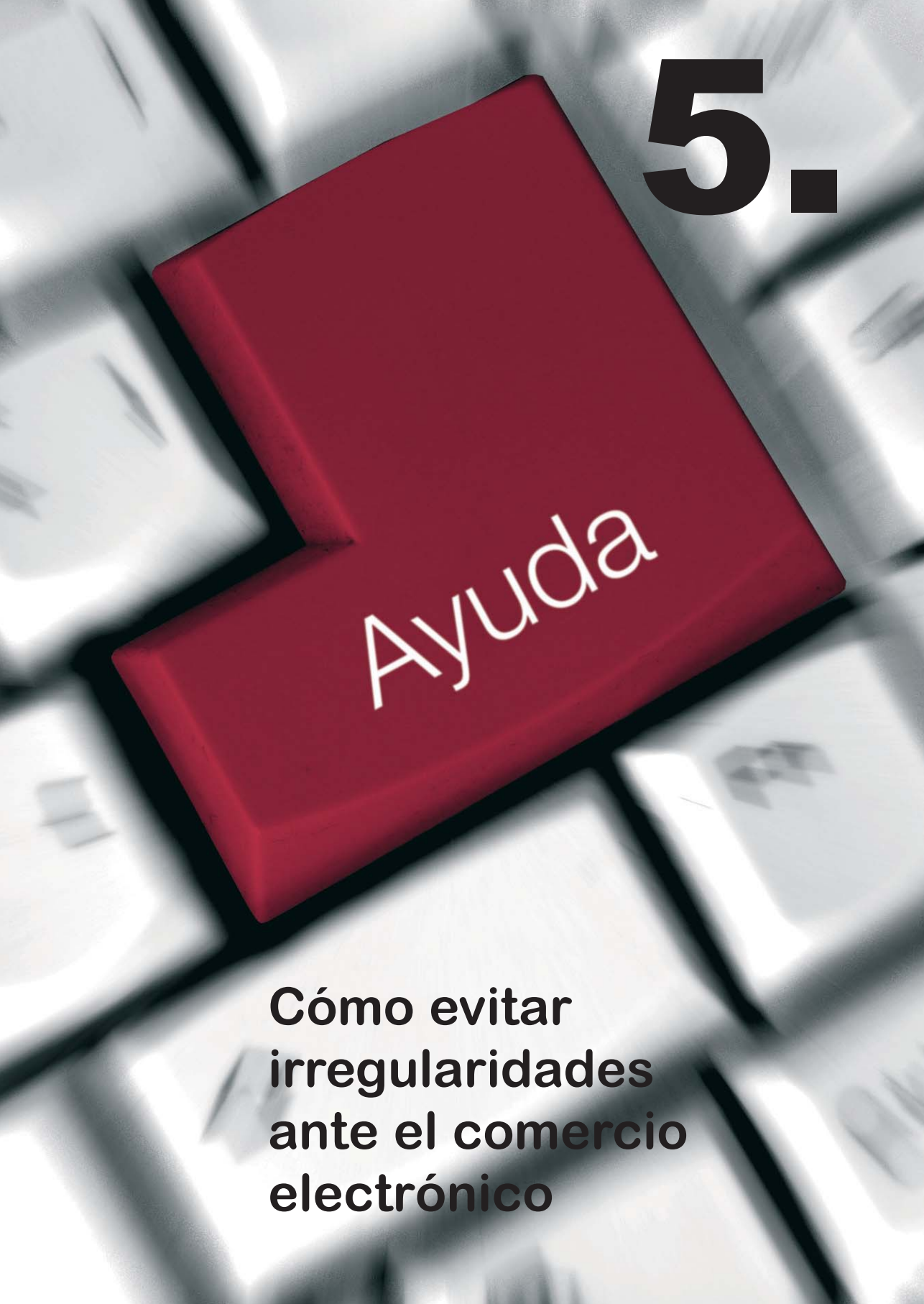
está procediendo a dar de alta una suscripción en boletines comerciales. Por ello es bueno capturar y almacenar las páginas en las que se ha efectuado algún tipo de operación y conservar todos los datos identificadores. Asimismo, los mensajes sospechosos deben ser leídos en formato texto y no en formato html y debe desactivarse la previsualización de los correos.

- Mantener al día el sistema informático, con un mantenimiento adecuado e incorporando las actualizaciones y parches que corrigen los problemas detectados en los programas. Dichas actualizaciones suelen estar disponibles en las propias páginas web de los fabricantes y su descarga e instalación suelen ser rápidas y gratuitas. Asimismo, es conveniente dotarse de un eficaz programa antivirus así como de cortafuegos para evitar la instalación de *software* malicioso.

- Hay que añadir que algunos filtros de correo funcionan efectivamente previniendo gran cantidad de *spam*, pero ninguno funciona lo suficientemente bien como para poder olvidar e ignorar estos simples consejos que, utilizados correctamente, ayudan a recibir menos correo no deseado. Además, otra característica negativa de los filtros es que algunos funcionan tan sensiblemente que terminan filtrando correo normal. Algunos de ellos son de pago.

- Por último, no se puede dejar de hacer mención en este apartado a los derechos de acceso o cancelación que tienen todos los usuarios sobre sus datos ante estas empresas. Estos derechos se encuentran regulados en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en el Reglamento 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo.

5.



Cómo evitar irregularidades ante el comercio electrónico

5 CÓMO EVITAR IRREGULARIDADES ANTE EL COMERCIO ELECTRÓNICO

Para evitar irregularidades frente al comercio electrónico es necesario extremar las precauciones para confirmar y asegurarse de la identidad del comercio en una transacción electrónica y para asegurarse de conocer todas las características de un producto que el consumidor no podrá examinar hasta que lo tenga frente a él.

También debe tenerse en cuenta si la empresa o comerciante de bienes y/o servicios que oferta su mercancía en Internet se encuentra o no ubicada en un país donde las garantías legales establecidas para el comercio electrónico no sean aplicables.

Por ello, es aconsejable no contratar con aquellas empresas que tienen sus domicilios sociales en paraísos legales y donde por tanto el consumidor tendrá serias dificultades de reclamar y exigir sus derechos si es engañado.

Toda oferta de compra por comercio electrónico deberá contener necesariamente la identidad y el domicilio social del proveedor, las características especiales del producto, el precio y, en su caso, el coste del transporte, así como las posibles formas de pago, la modalidad de entrega y el plazo de validez de la oferta. Debe exigirse toda la información necesaria sobre el producto por escrito para evitar sorpresas.

A modo de consejos prácticos debe tenerse en cuenta lo siguiente:

- Evitar contratar servicios o adquirir bienes a través del comercio electrónico cuando el comercio,

empresa o prestador del servicio no esté identificado o no se ofrezcan datos suficientes sobre los productos o servicios que permitan motivar la decisión de compra o contratación.

- Asegurarse del país en el que está ubicado el comercio y de que no se trata de un paraíso legal-fiscal donde no es de aplicación las normas de protección a los consumidores que rigen en la Unión Europea o similares.

- Antes de adquirir el producto o servicio accede y lee detenidamente las condiciones generales de contratación. Si no están accesibles, solicítalas para que te las envíen por escrito.

Exige que entre las condiciones se recoja un plazo de entrega y las consecuencias de su incumplimiento.

- Comprueba las garantías que te ofrecen: derecho de resolución y devolución del producto.

- Infórmate de los sistemas de entrega que la empresa tiene así como de los costes del mismo.

- Conserva todos los comprobantes de las compras que realices y revisa los extractos bancarios y los cargos por utilización de la tarjeta de crédito cuando abones las compras a través de este medio de pago.

- Comunica y anula los cargos que de forma irregular te hayan realizado en tu cuenta corriente.

- Comprueba que la empresa o el prestador del servicio permite una transacción segura, con garantía del uso de tus datos personales.

- Asegúrate de que la empresa cuenta con canales de reclamación y te informa de ellos. Igualmente, consulta si se encuentra adherida al Sistema Arbitral de Consumo.

- Utiliza un sistema de pago seguro.

- Guarda un registro de las transacciones: detalles de la página web, copias de los correos electrónicos enviados y recibidos del proveedor, 'pantallazo' de la página donde se confirma la transacción, etc.
- Comprueba cuanto antes que el producto recibido es exactamente el solicitado, y si está en buen estado y funciona correctamente.

RECLAMACIONES

En algunas ocasiones, pese a haber tenido en cuenta todos los consejos y recomendaciones y haber tomado todas las precauciones necesarias, el consumidor no está exento de recibir correos *spam*. En este caso, es necesario que los consumidores tengan conocimiento de cuáles son los cauces y los mecanismos de reclamación que en cada caso proceden.

Sobre este aspecto, la Ley General de Telecomunicaciones atribuye a la Agencia Española de Protección de Datos la tutela de los derechos y garantías de abonados (persona física o jurídica con contrato con el operador) y usuarios (quienes utilizan los servicios sin haberlos contratado) en el ámbito de las comunicaciones electrónicas, encomendándole la imposición de sanciones cuando en la prestación de los servicios de comunicaciones electrónicas se vulneren los siguientes derechos:

- A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.

- A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

- A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

- A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

- Además se garantizará a los abonados el derecho a no figurar en las guías ni en los servicios que informan sobre ellos.

Por otra parte, la Ley de Servicios de la Sociedad de la Información establece que corresponde a la Agencia Española de Protección de Datos la imposición de sanciones en el caso de infracciones por el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes que previamente no hubieran sido solicitadas o expresamente

autorizadas por los destinatarios de las mismas, salvo que exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

Asimismo, corresponde a la Agencia Española de Protección de Datos la imposición de sanciones cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales (*cookies*) sin informar a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito. Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

Las sanciones previstas en la Ley de Servicios de la Sociedad de la Información respecto del *spam* son también aplicables cuando no se respeta el derecho de los abonados a no recibir llamadas automáticas sin intervención humana o mensajes de fax con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

No obstante lo anterior, investigar los casos de *spam* se está convirtiendo en una tarea cada vez más complicada, en tanto en cuanto los spammers contratan piratas informáticos para ocultar su verdadera identidad (*spoofing*).

Los proveedores de servicios de Internet (ISP) suelen ser diligentes a la hora de cortar el servicio a los spammers cuando constatan que se generan correos basura desde sus redes. Por ello, si se tiene conocimiento del país a partir del cual se emite el *spam*, se debe indicar a las autoridades interesadas.

Tratándose de *spam* emitido en un Estado de la Unión Europea, los datos del conjunto de las autoridades europeas de protección de datos están disponibles en la página web de la AEPD. Por último, indicar que si el envío de *spam* se ha realizado desde los Estados Unidos de Norteamérica, pueden transferir los mensajes no solicitados al Departamento del Comercio Americano (Federal Trade Commission) que propone un procedimiento de alerta en su página web *cookies* y con el que la Agencia Española de Protección de Datos ha suscrito un acuerdo de colaboración.

Por ello, cuando un usuario reciba una llamada, mensaje o correo electrónico no deseado, debe actuar de la siguiente manera:

- Vía amistosa: en su caso, habría que interponer una reclamación a la empresa que haya vulnerado o infringido la norma con el fin de solicitar el cese de la misma y la cancelación de todos los datos de carácter personal de los que puedan disponer. Asimismo, y en el caso de que se haya producido algún tipo de daño o perjuicio, también tiene que ser reclamado.

- Vía administrativa: por otra parte, la correspondiente Reclamación-Denuncia a la Agencia Española de Protección de Datos, poniendo en conocimiento de la misma la infracción cometida.

- Vía arbitral: de escaso uso en este tipo de casos, ya que la mayoría de las veces se trata de empresas sobre las que ni siquiera se conoce su denominación o su domicilio social. La vía arbitral es un sistema extrajudicial de conflictos voluntario y gratuito que permite solucionar litigios con la misma fuerza que una sentencia judicial (carácter vinculante de las resoluciones).

- Vía judicial: en el caso de no haber llegado a resolver el problema a través de ninguna de las vías anteriores, quedaría siempre abierta la posibilidad de acudir a la vía judicial para resolver el problema.

Oficinas centrales
Bécquer, 28 - 41002 Sevilla
Teléfono del consumidor
954 90 90 90

consumidoresenaccion@facua.org
www.facua.org

Publicación subvencionada por

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, POLÍTICA SOCIAL E IGUALDAD
INC INSTITUTO NACIONAL DEL CONSUMO

Este proyecto ha sido subvencionado por el Ministerio de Sanidad, Política Social e Igualdad/Instituto Nacional del Consumo, siendo su contenido responsabilidad exclusiva de FACUA

Dep. Legal: SE-7214-2011

Publicación impresa en papel ecológico