

## ¿Qué es?

**Spam** son mensajes no solicitados, habitualmente propaganda enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico, aunque existen otras. El futuro del spam que ya es prácticamente presente, está empezando a cebarse con los teléfonos móviles a través de mensajería de texto.

## ¿Cuándo comenzó?

El spam mediante el servicio de correo electrónico nació el 5 de marzo de 1994., cuando la firma de abogados de *Canter and Siegel*, publica en un foro un mensaje de anuncio de su firma legal; en el primer día después de la publicación, facturó cerca de 10.000. Desde ese entonces, el marketing mediante correo electrónico ha crecido hasta convertirse en insoportable.

El **origen de la palabra spam** tiene raíces estadounidenses; una empresa charcutera Hormel Foods lanzó en 1937 una carne en lata originalmente llamada Hormel's Spiced Ham; El éxito del invento lo convirtió con el tiempo en una marca genérica, que hizo recortar el nombre, dejándolo con solo cuatro letras: Spam. Fue entonces cuando los [Monty Python](#) empezaron a hacer burla de la carne en lata, tenía la costumbre de gritar la palabra *spam* en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, que perturba la comunicación normal en internet.

## ¿Qué dice la Ley?

En nuestro país el spam está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), publicada en BOE 12 de Julio de 2002.

Aparte, a los poseedores de bases de datos de correos electrónicos se les podría aplicar la Ley Orgánica de Protección de Datos ([LOPD](#)) por tratarse de datos de carácter personal. De hecho, las sentencias en España referidas al spam están relacionadas con esta ley.

## Tipos de Spam

### *Spam por correo electrónico*

Es el medio más común de *spamming* en internet, aunque no el único. Consiste en enviar mensajes idénticos o casi idénticos a un gran número de direcciones. Se diferencia de otros correos publicitarios porque generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam.

### *Spam por mensajería instantánea*

Se le conoce como *spim*, utiliza los sistemas de mensajería instantánea como MSN Messenger. Los sistemas de mensajería ofrecen un directorio de usuarios, incluyendo información demográfica tal como edad y sexo. Esta información puede ser obtenida por los publicistas y hacer envíos masivos de correos para diferentes perfiles de usuarios. Para el envío masivo de correos solo se necesita software de scripting y los nombres de usuario de los receptores.

También este tipo de spam suele usarse en los canales de IRC usando lo que se llaman bots de IRC cuyo modus operandi es en primer lugar conectarse a los canales y bombardear con mensajes publicitarios. Debido a que la mayoría de los protocolos de mensajería instantánea son propietarios hace que este tipo de ataques sea más difícil para el spammer.

### *Spam en grupos de noticias*

Fue el padre del spam por correo electrónico, y suele realizarse en los grupos de noticias Usenet.; se define como *publicación excesiva de múltiples mensajes*, es decir, la publicación repetida de un mensaje (o mensajes sustancialmente similares). Dada que es un sistema en el que la publicación es muy sencilla los grupos de noticias son un objetivo popular para los spammers.

### *Spam en foros*

Suele definirse cuando en un foro de internet un usuario publica algo que no tiene nada que ver con el tema de conversación. También, en algunos casos, un mensaje que no contribuye de ninguna forma al tema es considerado spam. Una tercera forma de Spamming en foros es cuando una persona publica repetidamente mensajes acerca de un tema en particular en una forma indeseable (y probablemente molesta) para la mayor parte del foro.

### *Spam por telefonía móvil*

El spam por telefonía móvil está siendo una realidad y se da cuando recibimos un mensaje publicitario en nuestro teléfono móvil. Lo peor es que muchas veces deben pagar para recibir el mensaje de texto.

### *Spam por telefonía IP*

Este tipo de comunicaciones son vulnerables a ser spammeadas por mensajes pregrabados. Aunque los incidentes hayan sido escasos, si es cierto que las se están tomando las medidas oportunas

### *Spam en mensajería de juegos en línea*

Muchos juegos en línea permiten a los jugadores contactarse entre ellos via mensajería peer-to-peer o salas de chat. Estos servicios a veces suelen ser usados para promover ciertos sitios web y tiendas en línea, sin preocuparse por violar directamente el acuerdo de usuario final del juego, el cual prohíbe utilizar las comunicaciones dentro del juego para tales propósitos.

## Técnicas de spam

### *Obtención de direcciones de correo*

Los *spammers* (personas o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes.
- Los grupos de noticias usenet cuyos mensajes suelen incluir la dirección del remitente.
- Listas de Correos basta con apuntarse e ir anotando las direcciones de sus usuarios.
- Correos electrónicos con chistes, presentaciones divertidas con mensajes catastrofistas sobre el cierre de alguna página, supersticiones de mala suerte, sobre el amor, la amistad, etc. que los usuarios de internet suelen reenviar sin ocultar sus direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje y que son capturadas por un troyano o, mas raramente, por un usuario malicioso. Sin duda alguna esta es una de las técnicas más extendidas.
- Correos electrónicos que abusan de la buena fe de la gente, con solicitud de ayudas para alguna persona desaparecida, ayuda al tercer mundo.
- Correos electrónicos Páginas en las que se solicita tu dirección de correo (o la de "tus amigos" para enviarles la pagina en un correo) para acceder a un determinado servicio o descarga.
- Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal en servidores.
- Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Envío de los mensajes

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los *spammers* utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a internet, por consumirse gran parte del ancho de banda en mensajes basura.

#### *Verificación de la recepción*

Por norma general el *spammer* controle las direcciones correctas a través de web bugs que son pequeñas imágenes o similares contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del *spammer*, que registra automáticamente el hecho.

Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído. Si recibe un correo no solicitado debe borrarlo sin leerlo.

#### *Troyanos y ordenadores zombis*

Una de las técnicas más utilizadas. Los virus troyanos que se expanden masivamente por ordenadores sin cortafuegos. Los equipos infectados son utilizados por el *spammer* como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos de todo tipo, aunque los más preferibles son los correos cadena (FW) en busca de más direcciones. El usuario ignora haber sido infectado sin saberlo, al ser identificado como *spammer* por los servidores a los que envía spam sin saberlo suele acceder a determinadas páginas o servicios, incluso puede ser indicativo para el usuario.

#### *Servidores de correo mal configurados*

Los servidores de correo mal configurados son aprovechados también por los *spammer*. En concreto los que están configurados como Open Relay. Estos no

necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan los ordenadores que conectados directamente a Internet permiten su utilización por los *spammers*.

## ¿Cómo evitar el correo basura?

Si tienes que poner tu dirección en tu web para que contacten contigo:

- En vez de poner la dirección como texto, muéstrala en una imagen con la dirección de correo.
- En vez de poner el enlace a tu cuenta, usa una redirección (puede ser temporal o por un número de usos), y bórrala cuando recibas excesivo spam.
- Modificar la dirección para evitar el rastreo automático. Por ejemplo, cambiar "nombre@dominio.com" por "nombre (ARROBA) dominio (PUNTO) com", "nombre@dominioNOSPAM.com, quita NOSPAM" o "n0mbre@d0mini0.c0m (sustituir los ceros por oes)". Ayuda pero no es 100% efectivo.
- Una combinación de las anteriores.
- Algunos servicios de correo gratuito como Mailinator ofrecen cuentas temporales sin tener que usar contraseñas. Los mensajes se borran automáticamente al cabo de unas horas. Puede ser útil si sólo quieres que contacten contigo una vez, por ejemplo para confirmar un pedido.

En los grupos de noticias y foros:

- No poner el remitente verdadero en los post enviados.
- Si el archivo de mensajes a la lista es visible desde web, cambiar las direcciones de remite por una imagen, ocultarlas, o escribirlas de forma que sea difícil reconocerla como tal para un programa.
- Para evitar spam en una lista:
  - El foro puede estar moderado, para evitar mensajes inadecuados.

- Rechazar correos de usuarios no suscritos a la lista.

Otros:

- No reenviar mensajes parte de una cadena de correo electrónico
- No hacer envíos a amigos o colaboradores en los que aparezcan muchas direcciones y, si se hace, usar BBC (o CCO) para que no sean visibles las demás direcciones.
- Ten la precaución de que si reenvías un correo electrónico que ya contiene alguna dirección en el mensaje, asegúrate de borrarla.
- Al rellenar una inscripción no dar el correo. Si es necesario dar una dirección correcta (envío de contraseñas, confirmación de la suscripción, etc.) utiliza una redirección temporal, o una cuenta gratuita. En caso de que indiquen una recomendación del tipo "preferiblemente cuenta no hotmail", hacer caso omiso de las mismas.
- Leer los correos de remitentes sospechosos como texto, y no como html.
- No enviar nunca mensajes al *spammer*, aunque prometan dejar de enviar spam si se les pide. Normalmente suelen ofrecer una forma de anular la suscripción a su boletín de mensajes mandando un mensaje a una dirección de tipo unsubscribe@dominio.com. Si mandas un mensaje a dicha dirección con la esperanza de dejar de recibir correo no solicitado, sólo estás confirmando que tu cuenta existe y está activa, por lo que acabarás recibiendo *más* spam que antes.
- Tener siempre al día las actualizaciones de seguridad de tu sistema operativo, y programa de correo electrónico
- Instalar un antivirus y firewall (cortafuegos) instalado
- Hay formas de bloquear mensajes que tengan ciertas características, por ejemplo, si en el asunto aparece la palabra "porno", análisis de cabeceras, del texto del correo. Sin embargo, muchos spammers escriben algunas palabras modificaciones de una palabra por lo que no suele ser muy útil.
- Consultar y usar las listas negras públicas, creadas mediante la colaboración de varios usuarios.

- De servidores de correo o dominios (DNS) que se sabe que envían spam. Por ejemplo MAPS (mail-abuse.com) o ordb.org o spamcop.net
- De mensajes. Funciona de forma parecida a un antivirus, se crean resúmenes digitales (*hash*) de los mensajes de spam, y los mensajes recibidos se comparten en una base de datos. Ejemplo: Vipul's Razor