

# GUÍAS FÁCILES DE LAS TIC

del

**COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN**

**Trabajo Premiado 2006**

**Spam**

**Autor:**

**D. José Enrique Soriano Sevilla**

17 de Mayo 2006  
**DIA DE INTERNET**



colegio oficial  
ingenieros de telecomunicación

# spam

## ¿Qué es spam?

Todos nos hemos encontrado al llegar a casa alguna vez, el buzón lleno de folletos de publicidad que generalmente acaban en la basura por su poca o nula utilidad. Pues bien, de la misma forma, se puede definir el *spam* como mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada y en la que se centrará esta guía es la basada en el correo electrónico. Otras vías que se emplean para bombardear a los usuarios con publicidad no requerida son la telefonía móvil, la mensajería instantánea, los grupos de noticias, foros, juegos on-line, etc.

Los *spammers*, personas o empresas que realizan el *spam*, obtienen de esta forma una publicidad muy rentable, pues con un simple clic se logra hacer llegar el producto a millones de usuarios, siendo el coste de esta publicidad prácticamente nulo.

Este tipo de tráfico preocupa cada vez más a los usuarios y proveedores de Internet. Para dar una muestra del volumen de datos que supone el *spam*, actualmente, se calcula que entre el 60 y el 80% de los e-mails que se envían son de este tipo de publicidad no solicitada, con el consiguiente coste para usuarios y proveedores de servicio.

## Un poco de historia.

Antes de entrar en detalle con el funcionamiento del spam, buceemos un poco en el curioso origen de este término para definir el correo basura.

El origen de la palabra *spam* está en una popular carne en lata que se comercializó en Estados Unidos en 1937, Hormel's Spiced Ham. Esta carne, llegó a ser tan conocida que propio fabricante le recortó el nombre, dejándolo con solo cuatro letras: *spam*. El *spam* tuvo tal éxito que alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial y fue comercializado en todo el mundo.

Fue entonces cuando los Monty Python en un famoso sketch de su película Flying Circus comenzaron a hacer burla con esta palabra, repitiéndola hasta la saciedad en un contexto en que la palabra se refería a algo inútil y carente de sentido.

A raíz de esto, y de forma metafórica, se aplicó el término *spam* a aquellos correos electrónicos inútiles y vacíos de sentido para el receptor, pues, al no haberlos solicitado, contienen información que no le es de ningún valor.

## ¿Cómo funcionan los métodos de spam?

A la hora de realizar un buzoneo masivo de publicidad, el primer paso que se da es la obtención del correo electrónico de aquellos usuarios a los que va dirigida la campaña. Los *spammers* utilizan diversas técnicas para conseguir las listas de direcciones de correo que necesitan para su actividad. El medio más usado para esta actividad son los 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 y listas de correo. A los spammers les basta con apuntarse e ir anotando las direcciones de los remitentes.
- Correos electrónicos con chistes, cadenas, etc., que los usuarios suelen enviar sin ocultar las direcciones y que pueden acumular cientos de ellas, pudiendo luego ser capturadas por un troyano o cualquier receptor de la cadena.
- Páginas en las que se solicita tu dirección de correo para acceder a un determinado, como puede ser el envío de postales de felicitación.
- Compra de bases de datos de direcciones de correo. Pese a ser algo ilegal en la mayoría de países del mundo, pues los datos personales están protegidos, sigue siendo una forma rentable de obtener direcciones para el buzoneo.

Una vez que el spammer tiene una gran cantidad de direcciones de correo electrónico válidas, utilizan programas que recorren esta lista de direcciones enviando el mismo mensaje a todos los usuarios. Esto supone un costo mínimo para el spammer, pero perjudica de forma notable al receptor (pérdidas económicas y de tiempo) y, en general, a Internet, por consumirse gran parte del ancho de banda en mensajes basura.

Tras el envío de los correos, es frecuente que el *spammer* controle qué direcciones funcionan y cuáles no. Esta labor la realiza por medio de *web bugs*: 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, constatando que tras la dirección existe un usuario real. Otra forma ingeniosa de verificar si la dirección de correo es válida es prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos. Así, cuando el usuario contesta, significa no sólo que lo ha abierto, sino que lo ha leído. Un ejemplo es el siguiente texto en el que el spammer invoca una supuesta ley para dotar de mayor credibilidad al mensaje. "*Bajo el decreto S.1618 titulo 3ro. Aprobado por el 105 congreso base de las normativas internacionales sobre SPAM, un E-mail no podra ser considerado SPAM mientras incluya una forma de ser removido. Si desea ser borrado de nuestras Bases o no recibir nuestros Mails, reenvie este mail con el subject ELIMINAR y la direccion del mail donde lo recibió*".

Una vez el *spammer* confirma una lista válida de correos electrónicos, pasa a jugar con ella, vendiéndola a compañías que las usarán para enviar información de sus productos o enviando ellos mismos publicidad de productos de dudosa calidad o incluso tentando al usuario a dar claves o números de cuenta para cometer fraudes con ellas.

### *¿Qué dice la ley?*

Ante este panorama, cabe preguntarse qué dice la ley al respecto de las prácticas de *spam*. En España, el *spam* está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, publicada en el BOE de 12 de julio de 2002. Esta ley prohíbe el envío de correos comerciales que no hayan sido

solicitados expresamente. Además, los mensajes con contenido comercial deberán aclarar al usuario su carácter con la palabra "publicidad" en su encabezamiento.

Cuando los Prestadores de Servicio de la Sociedad de la Información requieran de los usuarios o clientes su dirección de correo deberán informarlos de manera clara de la opción de no recibir mensajes a través del correo electrónico de sus productos o servicios antes de finalizar el contrato. Asimismo, los destinatarios podrán revocar su consentimiento en cualquier momento sin coste alguno para ellos.

Las **sanciones** que contempla la LSSICE en caso de incumplimiento oscilan entre los 30.000 y 150.000 euros para infracciones graves. El organismo encargado de tramitar el expediente sancionador corresponde a la Secretaría de Estado de Telecomunicaciones y de la Sociedad de la Información

Además, a los poseedores de bases de datos de correos electrónicos se les aplica la Ley Orgánica de Protección de Datos (LOPD), por la cual se puede incurrir en delito con su correspondiente sanción en el caso en que se empleen los datos del correo electrónico de forma indebida para el envío de publicidad no autorizada por el usuario.

### *¿Cómo puedo protegerme?*

Está visto que la ley nos protege, sin embargo, en ocasiones, no es posible acabar con el *spam* y continúan llegando estos molestos mensajes inútiles al correo electrónico. Llegados a este punto, ¿qué puede hacer el usuario para evitar recibir estos mensajes además de denunciar los hechos? Aquí vienen algunos consejos que serán de mucha utilidad para no recibir *spam* en lo sucesivo.

Si somos creadores de una página web y hay que poner la dirección de correo electrónico para que cualquier persona pueda contactar con nosotros, habrá que tomar ciertas precauciones. La más adecuada y sencilla en este caso es, en vez de poner la dirección como texto, mostrarla en una imagen con la dirección de correo. De esta forma, se logra evitar el rastreo de direcciones que realizan los robots de los spammers para luego bombardearlos de publicidad inútil.

En los grupos de noticias y listas de correo electrónico, hay que ser cautos y no poner el remitente verdadero en los post enviados. Para ello, se pueden adoptar ciertas estrategias como cambiar nuestra dirección de correo por una imagen, ocultarla o escribirlas de forma que sea difícil reconocerla como tal para un programa (midireccionARROBAservidordecorreo.com).

Otra forma de tratar de evitar el spam consiste en no reenviar mensajes que sean parte de una cadena de correo electrónico, pues, como se ha visto, es una de las fuentes para obtener direcciones susceptibles de spam. Para esto, lo más sencillo es usar el cambio Bcc (CCO) para que no sean visibles las demás direcciones.

Hay que tener también cuidado a la hora de rellenar una inscripción y no dar el correo correcto si el sitio no nos ofrece confianza. Si es necesario dar una dirección correcta (envío de contraseñas, confirmación de la suscripción, etc.), lo mejor es emplear una redirección temporal, o una cuenta gratuita "extra" prescindible de las que se ofrecen en la mayoría de los portales de Internet. Para este fin, existen algunos

servicios de correo gratuito que ofrecen cuentas temporales sin tener que usar contraseñas. Los mensajes se borran automáticamente al cabo de unas horas. En este caso, puede ser útil si sólo quieres que contacten contigo una vez, por ejemplo para confirmar un pedido o registrarte en un foro.

También hay que estar alerta y no enviar nunca mensajes al *spammer*, aunque prometan dejar de enviar *spam* si se les pide, pues como se ha visto antes, lo único que hace este mensaje es confirmar que tu cuenta existe y está activa, por lo que acabarás recibiendo más *spam* que antes.

Finalmente, se pueden emplear numerosos programas que técnicas muy variadas para filtrar el correo basura del deseado. Son medidas paliativas, que no atacan directamente la raíz del problema, pero al menos ahorran al usuario el tiempo de hacerlo manualmente.

Se han desarrollado varias técnicas para separar el correo deseado del no deseado. Algunas se centran en las cabeceras del mensaje, otras en el cuerpo y otras en el mensaje completo. Los filtros más efectivos suelen utilizar varias técnicas:

- *Filtrado por campos del mensaje de correo electrónico.* Filtran el correo según la dirección o el dominio del remitente, o por la aparición de ciertas palabras en el asunto del mensaje.
- *Filtrado mediante listas negras,* creadas mediante la colaboración de varios usuarios. Estas listas las podemos configurar nosotros manualmente a lo largo del tiempo o tomarlas de ciertos dominios dedicados a ello, como pueden ser *www.mailabuse.com*, *www.ordb.org* o *www.spamcom.net*.
- *Filtros basados en el contenido.* Se basan en el estudio del mensaje en sí y suelen ser los más efectivos. La idea básica es que la mayoría del *spam* intenta transmitir unos mensajes muy concretos y con un tono muy particular, así que debe ser posible distinguirlos de los mensajes deseados que intercambia un usuario con otros. La mayoría de los utilizados actualmente se basan en un método de *filtrado bayesiano*. A grandes rasgos, consiste en contar las palabras que aparecen en una muestra de mensajes deseados y no deseados y asignarles una probabilidad en función de su frecuencia. Las que aparezcan más a menudo en mensajes no deseados tendrán una probabilidad alta de ser parte de un *spam*. Cuando llega un mensaje nuevo se calcula la probabilidad de que sea un *spam* según las palabras que tiene, y si pasa de un umbral (por ejemplo 90%) se considera *spam*. El algoritmo necesita un cierto volumen de correos clasificados como deseados y no deseados por el usuario para ser efectivo, cosa que puede hacerse indefinidamente. Cuantos más mensajes se utilicen como muestra mejor es la capacidad de detección. La gran ventaja de este método es que el filtro depende de los mensajes que reciba ese usuario, particularizándose para él, por lo que a la larga será mucho más efectivo que cualquier filtro genérico.

En cualquier caso, y usando la técnica de prevención y filtro que se desee, se debe informar a las autoridades y al webmaster del lugar que nos da alojamiento el correo para que así sea más fuerte nuestra lucha contra el *spam*.