

SPAM

Una amenaza real para el correo electrónico

GRETEL 2004

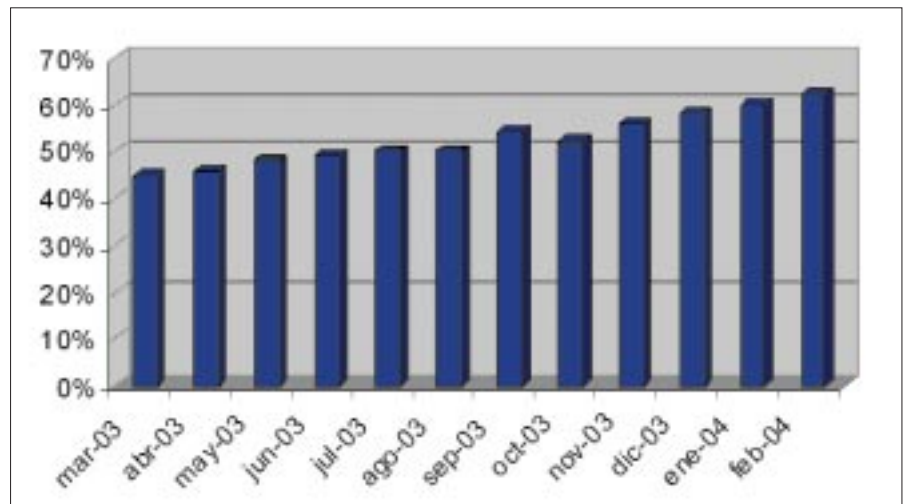
Con el crecimiento de Internet y el correo electrónico se ha producido también un fuerte aumento de los correos no deseados (spam). En estos momentos aproximadamente el 60% de todos los correos que circulan por Internet son correos no deseados por sus receptores¹. En España, el 90% de los internautas reciben spam, suponiendo ello una molestia para el 80% de los mismos².

La Figura 1 recoge la evolución en el último año del porcentaje de spam del total de e-mails de Internet.

Los correos no deseados son molestos, causan importantes problemas de seguridad, hacen perder tiempo, recursos y dinero a los usuarios, empresas y organizaciones, proveedores de servicios y de infraestructuras.

¿QUÉ ES EL SPAM?

La definición más aceptada para el término spam es: toda comunicación electrónica³ no deseada por su receptor con independencia del procedimiento empleado para su envío. Ofertas comerciales de todo tipo, timos, cartas encadenadas o correos con virus forman parte del paisaje que cada día nos dibuja el spam en nuestro e-mail. En la Figura 2 se presenta el peso relativo de los distintos contenidos del spam.



No obstante, es conveniente reconocer que el correo electrónico te nuevo medio, por lo que el uso de las comunicaciones electrónicas

Figura 1. Porcentaje de Spam del total de e-mails (ámbito mundial).
Fuente: AUI (Asociación de Usuarios de Internet) - Brightmail

es el medio de comunicación por excelencia en la Sociedad de la Información, por lo que muchas de las prácticas comunicativas del mundo real (lícitas y socialmente aceptadas) tenderán a trasladarse a es-

habrá de analizar, más tarde o más temprano, los contenidos y las formas utilizadas en estas comunicaciones.

Según el Radicati Group⁴, el spam tiene un coste para las empresas de

¹ Según algunas estadísticas de julio de 2003, alrededor del 50% de todo el tráfico de e-mails se consideraba spam, frente al 8% de mediados de 2001. Para más información véase el informe "Background Paper for the OECD Workshop on Spam" (22-Jan-2004).

² Según datos del Informe "La Sociedad de la Información en España 2003", Telefónica.

³ La Directiva 2002/58 CE sobre la Privacidad y las Comunicaciones Electrónicas define comunicación como "cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público".

⁴ Radicati Group, fundado en 1993, es una firma dedicada a los estudios de mercado, tendencias y previsiones desde una perspectiva global. <http://www.radicati.com/>

49 dólares por buzón y año, solamente en términos de equipamiento y comunicaciones, a lo cual habría que añadir lo que quita en productividad para los trabajadores. Por cada spam que llega al receptor, está calculado que éste pierde una media de 3 segundos en cada uno, si ponemos precio a este tiempo veremos que el coste para una organización al cabo del año es realmente importante. En este sentido, aunque sea difícil estimar la totalidad de los costes a nivel global, según los últimos estudios llevados a cabo por la UE, este coste puede alcanzar los 10 billones de euros al año⁵.

El spam tiene dos tipos de autores (spammers): aquellos que lo hacen por ganar dinero (publicidad⁶) y los que lo hacen por molestar o para divertirse (cartas en cadena, virus, rumores).

Los primeros tienen un canal de publicidad en el que los costes los paga el que recibe la publicidad y no el que la envía (increíble pero cierto).

Algunos estudios que han analizado la posible rentabilidad de lo que se ofrece vía spam hablan de que un spammer puede fácilmente generar 1000 euros por cada millón de correos que envía, algo que consiguen hacerlo en un tiempo inferior a una hora con un coste de conectividad inferior a 0,1 Euros. Si quieres triplicar el beneficio sólo tienes que triplicar el número de envíos.

La otra fuente de spam son los virus y los gusanos que están aumentando exponencialmente en los últimos meses. El 90% de los virus se propagan por e-mail y el 51% de las empresas han sufrido pérdida de información y problemas de seguridad como consecuencia de estos virus informáticos. Estos programas llegan a nuestro ordenador

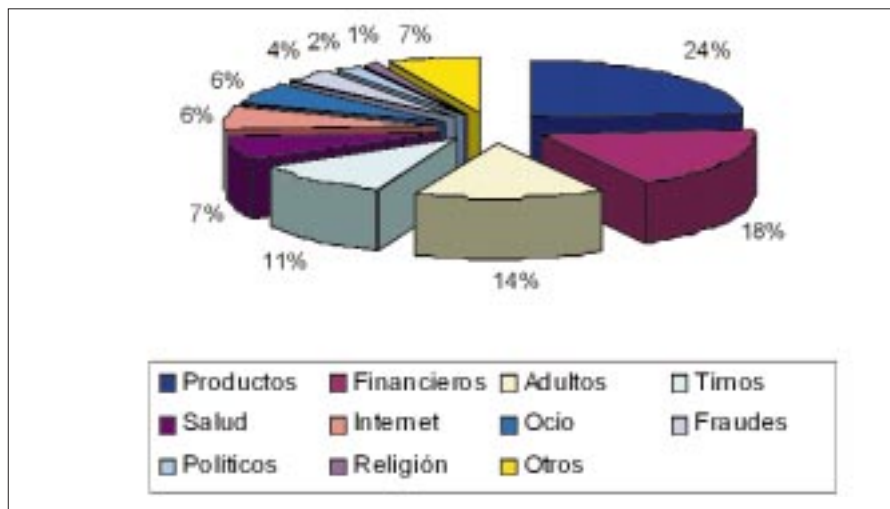


Figura 2. Tipos de Spam.

Fuente: AUI (Asociación de Usuarios de Internet) - Brightmail

vía e-mail y en general se envían desde nuestro ordenador a todas las direcciones de correo que tengamos en nuestra máquina.

Estos virus pueden ser destructivos para nuestro ordenador, pueden estar pensados para sacar información, para atacar a otros ordenadores o simplemente para molestar a todos nuestros conocidos. Tradicionalmente eran creados por hackers con afán de notoriedad, pero en estos momentos empiezan a converger y ya se dan casos de virus utilizados con fines comerciales similares a los que utilizan los anteriores.

Ya hay virus que cambian la publicidad que aparece en nuestro navegador (presentan ventanas no solicitadas, cambian los banners, envían recomendaciones a nuestros conocidos firmadas por nosotros) y todo esto desde el ordenador del usuario, el cual desconoce que esto esté pasando. Estos programas uti-

lizan reclamos como las descargas o el intercambio de ficheros y se aprovechan de las herramientas de intercambio P2P para conseguir una distribución masiva e incontrolada.

VULNERABILIDADES DEL CORREO ELECTRÓNICO Y PROBLEMAS GENERADOS POR EL SPAM

Los protocolos de correo electrónico actuales, y principalmente el de envío (SMTP- *Simple Mail Transfer Protocol*) presenta una característica que lo hace especialmente vulnerable, que es la facilidad que ofrece para falsificar el remitente y suplantar la identidad del que envía. Esto en una red globalizada es aprovechado por los spammers en general y por los estafadores en particular para burlar los controles y las investigaciones posteriores.

En este momento hay varias iniciativas en el plano técnico (SPF -

⁵ "Unsolicited Commercial Communications and Data Protection". Comisión Europea.

⁶ En este grupo sería discutible la actual inclusión de los pequeños empresarios que utilizan los medios electrónicos con fines de comercio lícitos en sus estrategias de comunicación así como a todas las comunicaciones de nuestra vida social y mercantil que se van trasladando al medio de comunicación por excelencia en la Sociedad del Conocimiento (el correo electrónico).

Sender Permitted From, Domreg, ..) de los servidores de correo, para que los ordenadores que envían e-mail estén registrados y para evitar que se utilicen remites falsos.

La otra debilidad deriva del bajo coste que tiene para el spammer el envío masivo, sobre todo si se usan recursos ajenos. Por ello otra de las líneas de trabajo de los servidores es controlar sus recursos y establecer unas políticas de uso que minimicen el riesgo de que se mal utilicen los recursos de un proveedor.

La solución de estas vulnerabilidades no elimina el spam, consiguen fundamentalmente evitar los abusos en recursos ajenos. Siempre queda la posibilidad de que alguien configure una máquina, que la registre y que se dedique a enviar correos de forma masiva desde un país que no persiga esta práctica.

Los problemas que genera el spam afectan a los siguientes agentes:

- El usuario receptor del correo spam, al cual le supone coste, molestia, tiempo y falta de seguridad.
- Los equipos que intervienen en las comunicaciones que deben gestionar un ancho de banda y un volumen de información, cuyo coste deberán repercutir al resto de agentes.
- Los proveedores de servicio de correo que tienen que aumentar el tiempo de proceso, la capacidad de almacenamiento y además desarrollar técnicas de filtrado que en algún caso pueden generar problemas adicionales con sus clientes (eliminar correos buenos, invadir la privacidad, ...).
- Los remitentes cuya identidad ha sido suplantada y que de repente se ven inmersos en un grave problema, que en algunos casos les puede llevar a tener que cambiar su cuenta de correo.

EL GRETEL DESTACA

- Estamos ante un problema de gran calado por su dimensión económica, social y funcional.
- No hay soluciones mágicas por lo que hay que actuar en todos los niveles de la cadena (usuarios, proveedores, reguladores, COIT y webmasters) y para ello hay que trabajar fundamentalmente en la coordinación del sector en España con otras de proyección supranacional.
- El objetivo es informar, sensibilizar y poner en marcha herramientas, soluciones y políticas que eleven la calidad en todos sus eslabones de la cadena y si es posible, de forma coordinada para aumentar la eficacia.
- Dotar a los proyectos de procedimientos técnicos normalizados para poder ajustarse a las normas, procedimientos y políticas que el sector decida poner en marcha en cada momento.
- Avanzar para incorporar la firma electrónica en el uso del correo electrónico como elemento que permite elevar la calidad y la seguridad en toda la cadena de valor a través de la identificación del remitente.
- Será necesaria una regulación de los contenidos, las prácticas y los métodos de envío de comunicaciones electrónicas, de acuerdo con la proporcionalidad del problema.

¿HAY SOLUCIONES PARA EVITAR EL SPAM?

Podemos decir que no hay una solución definitiva, pero sí hay medidas que se puede poner en marcha en diferentes niveles para ir incorporando al correo electrónico del nivel de calidad (seguridad, confidencialidad y disponibilidad) que necesita.

En el ámbito legal lo importante es conseguir que cada vez haya más países que regulen este tema y que haya una buena coordinación entre ellos para que cada vez sean menos los sitios desde los cuales haya impunidad para el envío de spam. En este sentido, indicar que hay dos tendencias en el mundo a la hora de regular el envío de correo publicitario: la de aquellos que obligan a que haya un consentimiento previo (*opt-in* para poder enviar e-mail) y la de aquellos que optan por lo contrario, que haya listas de exclusión (*opt-out*) a las que cualquiera se pue-

de apuntar y a la que todos los que envían deben de consultar.

En cualquiera de los casos la aplicación de la ley debe ir acompañada de mecanismos muy ágiles que faciliten la comunicación de este tipo de abusos. Lo ideal es que una denuncia de spam fuese cuestión de un click.

Los usuarios y los que generan los contenidos deben ser conscientes de los riesgos que se esconden detrás de una dirección de correo electrónico. Necesitan, por tanto, estar informados y sensibilizados para prevenirlas y disponer de canales sencillos y efectivos para comunicarse con su proveedor o con las autoridades para resolver su problema si ya es víctima del spam.

Por otro lado, hay medidas técnicas. Nos interesa distinguir entre aquellas que pueden ponerse en marcha antes de que el correo salga de su origen, antes de aceptarlo por el que gestiona el buzón destinatario del correo y, finalmente, las que se ponen en marcha una vez

aceptado antes de que el usuario lo reciba.

Las primeras son las más efectivas puesto que consideran el problema en su origen y evitan que se genere tráfico y carga a terceros. En esta línea hay que incluir todas las técnicas de seguridad, autenticación, control de flujo, remitentes, recursos y políticas de uso.

En el segundo plano están aquellas en las que el mensaje llega hasta el servidor que tiene el buzón receptor y que básicamente consisten en la gestión de listas negras (sitios desde los que no se recibe ningún mensaje), listas blancas (se aceptan todos los mensajes de estas direcciones) y más recientemente el control del registro de la máquina que inició el envío. Todas estas técnicas tienen ventajas e inconvenientes y en general son objeto de ataques de los spammers para hacerlas ineficaces.

Finalmente están las medidas técnicas que podemos poner en marcha una vez que hemos aceptado el mensaje. Estas medidas pueden implementarse bien en el servidor que aloja el buzón del receptor o en el programa del usuario que lee el correo. Las medidas más conocidas son la gestión de listas (blancas y negras) y el filtrado que puede ser con reglas fijas o adaptativo.

En general los proveedores utilizan combinaciones de diferentes técnicas, fundamentalmente filtrado y listas. Siempre que aparece una técnica el spammer inventa una forma de enviar el mensaje que despista o anula a los detectores. Por ejemplo en estos momentos encontramos correos que aprovechan el formato HTML para combinar textos aleatorios entre las letras de forma que se lee correctamente pero despista a los filtros adaptativos ya que cada mensaje es distinto a pesar de que se visualiza siempre igual.

Cuadernos GRETEL 2004

El Nuevo Marco Europeo de las Comunicaciones Electrónicas y su Implantación en España

GRETEL 2004

El GRETEL acaba de inaugurar una nueva temporada. El pasado 12 de febrero tuvo lugar la presentación de dos nuevas publicaciones -estrenando un nuevo diseño basado en formato de cuaderno, más dinámico y ágil para un sector cambiante necesitado de opinión profesional en el momento adecuado-, con lo que se retoma el sendero marcado por el último trabajo que realizó el GRETEL, dedicado al *"Nuevo Diseño Europeo de las Telecomunicaciones, el Audiovisual e Internet"*, para analizar el impacto del "nuevo marco regulatorio de las comunicaciones electrónicas" sobre el desarrollo del sector.

Esta nueva entrega, bajo el título general *"El Nuevo Marco Europeo de las Comunicaciones Electrónicas y su Implantación en España"*, se ha dividido en tres partes diferenciadas con el objeto de abordar todos los elementos clave que introduce la aplicación práctica de la nueva regulación.

El primero de los cuadernos tiene por título *"Análisis de la Nueva Regulación Europea de las Comunicaciones Electrónicas"* y pretende presentar al ingeniero de telecomunicación y al profesional los principales cambios que supone la implantación de los principios establecidos por el nuevo entorno de regulación de las telecomunicaciones en Europa, analizando aquellos aspectos de mayor relevancia.

El segundo cuaderno, *"La Transposición del Nuevo Marco Regulatorio Europeo de las Comunicaciones Electrónicas en España"*, se centra en el caso específico de España, haciendo una descripción de la nueva Ley General de Telecomunicaciones e incluyendo los ya famosos comentarios posicionales del GRETEL.

En el tercer cuaderno, *"Definición y Análisis de los Mercados de Referencia"*, se recoge en detalle una de las novedades más importantes del nuevo marco, que es el proceso de definición y análisis de los mercados relevantes del sector por parte de las agencias nacionales de reglamentación.

