1. Introducción

Uno de los grandes problemas que afronta actualmente Internet es la proliferación del correo basura, correo no solicitado, o no deseado y que no aporta ningún beneficio al receptor. Según algunas estadísticas, el correo basura constituye ya la mitad de todo el correo electrónico de Internet, y hasta el 80%, según la empresa especializada **MAPS**[1].

El correo basura **cuesta dinero** por dos razones principales:

- **el tiempo que se pierde:** la cantidad de estos mensajes que circulan puede hacerte perder mucho tiempo, no ya leyéndolos (algo que se deja de hacer enseguida, al comprobar que todos son similares), sino eliminándolos;
- **los recursos de hardware y software** necesarios para manejarlo (ancho de banda, servidores de correo más potentes, software de filtrado, etc.).

Estos costes deben ser soportados por las organizaciones en forma de inversiones y horas de trabajo de sus empleados, y, en el caso de los proveedores de acceso a Internet, acabarán repercutiendo a los clientes.

Además de que el correo basura implica costos de tiempo y dinero, aunque no sea lo más habitual, puede contener virus u otros códigos maliciosos, o direcciones de Internet que apunten a páginas web que estén preparadas para descargar (de manera no autorizada) algún tipo de programa en el equipo.

Si tenemos en cuenta que las 3/5 partes del correo entrante es correo basura, es fácil deducir qué ocurre con el ancho de banda: que sus 3/5 partes están ocupadas procesando correo no deseado. La consecuencia es una **ralentización en el acceso a Internet**.

También es puramente incidental que el spam sea usualmente comercial. Si alguien comenzara a enviar correos electrónicos en masa para apoyar alguna causa política, por ejemplo, éstos serían spam, tanto como lo puede ser el correo electrónico promocionando un sitio pornográfico.

Además de todo esto, existe el problema de la falsificación de direcciones de e-mail. Es muy fácil enviar un mensaje con cabecera *nicanor@mburuvicharoga.gov.py* y el receptor no tiene forma alguna de verificar las credenciales, salvo si examina las propiedades de la cabecera u obliga a sus amigos a enviar sus mensajes cifrados y firmados. Los últimos gusanos de Internet, se apoderan de la Libreta de direcciones de un usuario infectado y se reenvían, suplantando la identidad del origen, de tal manera que los receptores del virus creen estar recibiendo un mensaje de un conocido cuando se trata de una clara suplantación de identidad.

Existen y se están desarrollando técnicas para reconocer el spam y así poder eliminarlo automáticamente. A medida que estas técnicas vayan mejorando el correo electrónico volverá a ser una herramienta fantástica, como ninguna otra, que nos permitirá comunicarnos a un costo bajísimo.

[1] http://www.mail-abuse.org/cgi-bin/lookup

2. Definición de SPAM

Al **SPAM** se lo suele definir como correo electrónico no solicitado o no deseado que se envía a múltiples usuarios con el propósito de hacer promociones comerciales o proponer ideas. SPAM **también es conocido como e-mail comercial no solicitado**.

Desde nuestro punto de vista al spam **no sólo** se lo puede definir como correo electrónico comercial no solicitado. Por ejemplo, si nos enteramos que alguien en el vecindario está en busca de un auto en buen estado, y queremos hacerle una oferta, podemos enviarle un correo electrónico ofreciéndole la venta de uno, suponemos que esta persona estaría interesada, y aun así este correo electrónico **sería tanto comercial como no solicitado**.

Un mensaje electrónico se considera "Spam" si:

1. Se envía de manera **masiva y automatizada**, sin atender a la identidad ni al contexto del receptor.

   Los spammers utilizan mecanismos automatizados para enviar en forma masiva los e-mails. Esto se diferencia del ejemplo dado anteriormente, en el que nosotros enviamos un mensaje de manera personal, a un conocido en particular interesado en algo que podemos ofrecerle. Esto sin duda no es masivo, ni tampoco automatizado.

2. El receptor **no ha solicitado o permitido expresamente** de forma verificable el envío del mensaje.

   Si uno compra algo de una compañía, eso no implica que uno haya solicitado el envío indiscriminado de correo electrónico por parte de ellos. Si ordena algo de una tienda en línea, y luego ellos le envían un río de correo, esto sigue siendo spam.

   Las compañías que envían spam frecuentemente ofrecen una manera de "cancelar la suscripción", o piden que visite su sitio web y cambie sus "preferencias de cuenta" si desea que dejen de enviarle spam. Esto no es suficiente para que el correo deje de ser spam. **No cancelar un servicio no es lo mismo que pedir un servicio**. A menos que el receptor de los mensajes haya habilitado explícitamente una caja claramente etiquetada (cuyo valor por defecto haya sido *no*) pidiendo el envío de los correos, entonces es spam.

Definimos entonces al SPAM como:
Correo electrónico enviado de forma automatizada y masiva, que no fue solicitado o no es deseado por quien lo recibe.

3. Origen del término spam

El **origen de la palabra spam** tiene raíces norteamericanas con unas curiosas derivaciones socio-culturales.

La empresa charcutera norteamericana Hormel Foods lanzó en 1937 una carne en lata originalmente llamada *Hormel's Spiced Ham*. El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con solo cuatro letras: "SPAM". Este fue el primer producto de carne enlatado que no requería refrigeración. Esta característica hacia que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial.

Fue entonces cuando los **Monty Python** empezaron a hacer burla de la carne en lata. Su divertidísima costumbre de gritar la palabra SPAM en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado o querido que perturba la comunicación normal en Internet. En un famoso sketch[2] los comediantes representaban a un grupo de hambrientos vikingos atendidos por solícitas camareras que les ofrecían "huevo y panceta; huevo, salchichas y panceta; huevo y spam; huevo, panceta, salchichas y spam; spam, panceta, salchichas y spam; spam, huevo, spam, spam, panceta y spam; salchichas, spam, spam, panceta, spam, tomate y spam, ...". La escena acababa con los vikingos cantando a coro "Spam, spam, spam, spam. ¡Rico spam! ¡Maravilloso spam! Spam, spa-a-a-a-a-am, spa-a-a-a-a-am, spam. ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! Spam, spam, spam, spam".

Como la canción, el spam es una repetición sin fin de texto de muy poco valor o ninguno, que aplicado a los mensajes electrónicos, se refiere a los mensajes enviados de forma masiva y dirigidos a personas que, en principio, no desean recibirlos.

4. Historia del spam

Hace diez años, nacía el spam tal como lo conocemos. El 5 de marzo de 1994, una firma de abogados llamada *Canter and Siegel* envió un mensaje a unos cuantos grupos de noticias de Usenet, promocionando sus servicios para el Green Card lottery en EE.UU. Suena bastante pacífico hoy día, pero en aquel momento, ese movimiento y sus consecuencias provocaron indignación a través de la red. Atreviéndose a hacer lo que nadie había hecho antes, esos primeros mensajes de spam abrieron una puerta a la avalancha que batallamos diariamente. Cuando quedó claro que Canter y Siegel continuaba con sus mensajes, que no eran ni bloqueados ni ignorados, pronto otros siguieron sus pasos.

Como recordará cualquier persona que haya usado Internet hace 10 años, la ola de spam de Usenet que se derivó destruyó la utilidad de los grupos de noticias. Esto hubiera sido suficientemente malo, pero la cosa no terminó ahí. El siguiente desarrollo crítico fue cambiar el spam de los grupos de noticias de Usenet al spam a direcciones de correo electrónico individuales. La limitación inicial del spam a direcciones de correo fue la dificultad de juntar grandes listas para compensar la pequeña tasa de respuesta. Probablemente no sea coincidencia que la práctica del spam aumentó en el momento en que Internet se convertía en un medio masivo.

[2] http://bau2.uibk.ac.at/sg/python/Scripts/TheSpamSketch

5. ¿Por qué se envía tanto spam?

Por diversión. Existen personas que lo hacen por molestar o para divertirse (cartas en cadena, virus, rumores).

Es un negocio. La mayor parte de estos mensajes son campañas de publicidad engañosas (como productos milagrosos), fraudulentas (por ejemplo, colecciones de programas pirateados), o productos de baja calidad para los que no es rentable una campaña publicitaria convencional. La mayoría de los usuarios los perciben como tales, y aunque se estima que la tasa de respuesta es ínfima (menos de 15 por millón), debido al bajo coste que tienen, es suficiente para producir beneficios. Hay muchas personas y empresas que recurren a esta práctica y hay abundante información sobre cómo hacer spam[3] en Internet.

Aunque se hacen grandes esfuerzos para dificultarles su labor, los *spammers* (personas u organizaciones que envían spam) no permanecen pasivos y utilizan numerosas técnicas y trucos desarrollados en los últimos años para seguir entregando sus correos. Estas incluyen:

- Utilizar una dirección distinta para cada envío y abandonarla o eliminarlas después
- Falsificar las cabeceras de los mensajes de correo electrónico para dificultar el rastreo del origen.
- Infiltrarse en servidores de correo legítimos (reventarlos) y usarlos como fuente de envío.
- Utilizar troyanos, que pueden ser usados para reenviar spam.
- Deformación de palabras de los mensajes (por ejemplo cambiando letras por números, o insertando espacios y puntos aleatoriamente) para engañar a los filtros de palabras.

6. ¿A quiénes afecta el spam?

- Al 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 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.

[3] http://www.paulgraham.com/howspam.html

7. ¿Cómo funciona el spam?

La pregunta que muchos usuarios se plantean es: si yo no he autorizado a nadie para que me envíe estos correos y si, además, no les he dado mi dirección... ¿cómo es posible que la conozcan?

La respuesta es sencilla. Cuando se envía un correo electrónico, lo que se hace es enviar algo más **parecido a una postal** que a una carta. El contenido del e-mail está expuesto a cualquiera que reciba por error el mensaje o a cualquiera que lo intercepte. Esta postal puede pasar por múltiples servidores y redes que la pueden leer y, por supuesto, está suficientemente identificada para saber quién la ha enviado.

En la cabecera de cada e-mail que se envía están escritos los datos que permiten que el mensaje llegue a sus destinatarios. Por otra parte, en Internet no existe un único servicio de correo, sino miles de ellos. A priori es imposible que uno sepa por cuántos servidores, pasará el correo hasta llegar a destino, pero cada uno de ellos dejará su huella en el mensaje.

En esa cabecera, accesible a todos los ordenadores por los que va pasando, quedan grabados los siguientes datos:

- el programa con que fue escrito el mensaje
- la fecha
- el asunto
- a quién va dirigido
- quién lo manda y qué identificador tiene ese correo
- los servidores por los que ha pasado, incluyendo los del emisor y el del destinatario.

En pocas palabras: el IP y la dirección de correo están perfectamente visibles y hay gente malintencionada a la que interesa esa información.

8. ¿Cómo luchar contra el spam?

El spam tiene, generalmente, una serie de características que lo hacen relativamente fácil de identificar. Describimos tres mecanismos para lidiar con el **correo basura**.

1. Prevención: como en tantas otras cosas, más vale prevenir que curar. Los consejos básicos son:

- Utilice al menos dos direcciones de correo electrónico (o un alias). Una para sus contactos más importantes, y otra (u otras) para dar en sitios web o listas de correo, de forma que si empieza a recibir mucho correo basura pueda desechar esa dirección.
- Evite que su dirección de correo aparezca en sitios web, donde son muy fáciles de capturar, especialmente si se usan enlaces de tipo *mailto:*
- Procure no participar en mensajes encadenados que son remitidos masivamente a numerosos destinatarios en el campo "Para". Recomiende a sus contactos que usen el campo "CCO" (Con Copia Oculta) o que usen listas de distribución de correo.
- Nunca responda al spam, a no ser que esté convencido de que proviene de una fuente seria. La dirección del remitente suele ser falsa, así que si devuelve el correo, probablemente le llegue a alguien que no tenga nada que ver. Las instrucciones para no recibir más mensajes similares también suelen ser falsas, y normalmente lo único que se consigue es confirmar al *spammer* que la cuenta está activa y recibirá más correo basura. Y por supuesto, no adquiera nunca productos anunciados mediante spam para no sustentar estas prácticas.

2. Denuncia. Denuncie a las autoridades competentes el envío de spam y participe en la **creación de listas negras**. También puede enviar correo a las cuentas *postmaster* o *abuse* de los servidores de correo por los que ha pasado el mensaje, aunque sólo el último (registrado por nuestro servidor de correo) es fiable. Esta información aparece en las cabeceras del mensaje.

Informe a su proveedor de Internet de aquellas personas o empresas que envían spam.

3. Utilización de **filtros anti-spam**. Se han desarrollado numerosos programas que usan varias técnicas para separar el correo basura del deseado. Son medidas atenuantes, que no atacan directamente la raíz del problema, pero al menos ahorran al usuario el tiempo de hacerlo manualmente.

4. Otras medidas **SPF y CallerID**. Evitan recibir correo de direcciones de e-mail que han sido falsificadas por los spammers evitando la molestia de recibir y borrar el correo basura.

9. Técnicas anti-spam.

Se han desarrollado varias técnicas para filtrar el correo no deseado. Las técnicas pueden basarse en el control de:

- la cabecera del mensaje;
- el cuerpo del mensaje;
- y otras en el mensaje completo.

Los filtros más efectivos suelen utilizar varias técnicas.

- **Filtrado por campos** del mensaje de correo electrónico. La mayoría de los clientes de correo electrónico permiten clasificar el correo según la dirección o el dominio del remitente, o por la aparición de ciertas palabras en el asunto o en el cuerpo del mensaje. Estos filtros pueden eliminar un pequeño porcentaje de spam, pero los *spammers* los derrotan con facilidad falsificando las cabeceras del mensaje y modificando las palabras más relevantes. Además, exigen una configuración totalmente manual. Su mayor utilidad es la creación de listas blancas de remitentes conocidos, cuyos mensajes podrían ser considerados spam por otros métodos.

- **Análisis de cabeceras**: búsqueda de datos falsos en las cabeceras, incluyendo comprobación de que existe la dirección del remitente, si hay campos malformados, entre otros.

- **Listas negras públicas**, creadas mediante la colaboración de varios usuarios: Son una forma de controlar el correo basura a nivel del servidor. El servidor de correo, que se encarga de enviar y recoger el correo enviado y depositarlo en la casilla del usuario correspondiente, puede ser configurado para *ignorar los e-mails que vengan de una lista de direcciones IP que se suponen origen del correo basura*. Estas listas se obtienen a través de organizaciones que las actualizan constantemente, y las ofrecen gratuitamente como fuente de información sobre focos negros de spam. Hay que tener en cuenta que los spammers se sirven de servidores mal configurados para realizar sus envíos masivos, aprovechando recursos de terceros para intentar no ser detectados. Por tanto, si alguien se percata de la dirección de origen del abuso, puede dar cuenta a estas organizaciones, que la incluirán en sus listas negras, previniendo a todos los administradores que utilicen esta técnica, de esos correos no deseados. Algunas listas negras podemos encontrarlas en SpamCop[4], MAPS, Open Relay[5].

- **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 peculiar, así que debe de ser posible distinguirlos de los mensajes deseados que intercambia un usuario con otros.

    - **Filtros bayesianos**: Representan lo último en filtros antispam. Se basan en las teorías del matemático Thomas Bayes (1701-1761).

      A grandes rasgos, consiste en un programa que cuenta las palabras que aparecen en una muestra de mensajes deseados y no deseados y asigna una probabilidad en función de su frecuencia. Las que aparezcan más a menudo en mensajes no

[4] http://spamcop.net/bl.shtml
[5] http://www.ordb.org

deseados tendrán una probabilidad alta de ser parte de un spam. Cuando llega un mensaje nuevo calcula la probabilidad de que sea un spam según las palabras que tiene, y si pasa de un umbral (por ejemplo 90%) lo considera como spam. El algoritmo necesita un cierto entrenamiento en forma 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. Una ventaja derivada del entrenamiento del filtro por el usuario es que el filtro depende de los mensajes que reciba ese usuario, por lo que a la larga será mucho más efectivo que cualquier filtro genérico. Es decir, se puede tener un filtro personalizado. En resumen es una regla matemática para "aprender" y "realimentarse" de la experiencia diaria y establecer una nueva evidencia que reafirme o suavice una opinión[6].

- **Filtros heurísticos:** Los cuales buscan contenidos típicos de spam, como formularios HTML o identificadores únicos en el mensaje. Se basa en la propia experiencia del que lo sufre. Si por ejemplo se detecta que muchos correos contienen letras en rojo, añaden una nueva regla a su filtro que descartara estos mensajes. Esta técnica puede resultar efectiva, pero resulta tediosa, y las técnicas cambian tan rápido que es imposible seguirles el ritmo para mantener esa eficacia.

- **SPF (Sender Policy Framework)**: Lucha con la falsificación de direcciones de e-mail y hace que sea fácil la identificación de spams, gusanos y virus. Los dueños de un dominio identifican los servidores que mandan el mail en el DNS. El receptor que utiliza el protocolo SMTP[7] verifica la dirección de quien envía, y puede distinguir cuales son mails legítimos y cuales son spams, antes de que cualquier mensaje de datos sea transmitido.

[6] Ver Apéndice A para mayores referencias sobre este Filtros Bayesianos.
[7] Simple Mail Transfer Protocol

10. SPF

Falsificación de emails

Todo spam tiene un costo para las personas que lo reciben, pero el spam falsificado tiene un costo mucho mayor para las personas cuyas direcciones son falsificadas. Los ISP pueden incluso cerrar sus cuentas. Esto puede pasarle a muchas personas que no son spammers e incluso pueden no enterarse de lo que está sucediendo.

Es muy difícil conocer la identidad de quienes falsifican emails porque los spammers pueden ocultar su identidad de muchas maneras. En realidad es muy poco lo que se puede hacer cuando no se sabe quién envía realmente el mensaje.

¿Qué es SPF?

SPF (Sender Policy Framework) **es un protocolo**, y es la última iniciativa para combatir el spam. Intenta averiguar si existe una falsificación de identidad en los mensajes recibidos, con sólo examinar sus cabeceras.

SPF es un **protocolo abierto** como lo son SMTP y HTTP. Por su parte Microsoft está intentando imponer su norma, el protocolo **Caller-ID**, muy similar al SPF, salvo en que usa para el almacenamiento de información en los DNS código XML. El inconveniente es que Microsoft parece haberse olvidado que los registros DNS tienen un límite de 512 bytes en los datos almacenados. Y todos sabemos que para escribir un simple "Hola mundo" en una página web XML se requieren bastantes líneas de código, demasiados caracteres que hacen de este tipo de páginas algo muy pesado.

Al margen del peso de XML en HTTP, Microsoft consciente de las limitaciones del DNS en UDP, propone que las entradas DNS se hagan sobre TCP, teniendo así un límite de 2.000 bytes para los datos.

Los dos frentes más popularizados son SPF y Caller-ID. Caller-ID cuenta con más desventajas, aparte del propio uso de XML. Por ejemplo, **Caller-ID descarga un mensaje por completo antes de decidir si es spam. SPF sólo lee la cabecera.** Esto se traduce en que **con Caller-ID hay todavía más consumo de ancho de banda y CPU**. Teniendo en cuenta que las etiquetas XML ocupan más espacio que la propia información, es absurdo pensar en que los registros MX, A, PTR y CNAME deban codificarse a partir de ahora en XML.

Por si fuera poco, Caller-ID implica que se han de codificar las rutinas de búsquedas DNS para la ejecución de múltiples búsquedas recursivas. O sea, un nuevo gasto inaceptable en velocidad.

Parece ser que Microsoft se empeña en implantar Caller-ID, simplemente porque contiene XML, directamente relacionado con el uso de varias patentes de la compañía. Y aunque por el momento dice que no cobrará a nadie por utilizar Caller-ID, la desconfianza de los fabricantes es grande. Así que Microsoft sólo ha implementado Caller-ID en Exchange, y ha impuesto una fórmula para compatibilizar Caller-ID con SPF.

¿Cómo contraataca el SPF?

Pobox[8] se ha unido con líderes de la industria como Microsoft y AOL para introducir SPF, una propuesta para detener la falsificación de emails, para hacer que los spammers envíen emails desde sus dominios reales, en vez de secuestrar las cuentas de usuarios inocentes.

SPF permite a los dominios decir qué computadoras están habilitadas para enviar emails como dichos dominios. Si tu dominio usa SPF, y alguien trata de enviar un email haciéndose pasar por ti en Rusia (asumiendo que tu ISP no está en ese lugar), el ISP receptor puede rechazar el mensaje.

La mejor parte es que el usuario dueño de la cuenta no tiene que preocuparse. El administrador del dominio (ya sea un ISP, una escuela, su negocio, etc.) establece los remitentes aceptables. Quien reciba el mail se encarga de hacer el control. Para los usuarios, SPF es un proceso transparente, protegiendo la dirección de email sin problemas mayores.

El proceso

Como ejemplo, **AOL.com** es el dominio que envía el mensaje, y **pobox.com** es el receptor. **AOL** publica un **registro SPF**, especificando cuáles computadores (servidores de correo) en Internet pueden enviar mails como user@aol.com.

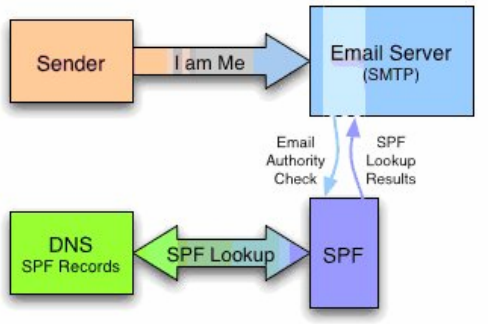
Mensaje de un usuario real.

1. Cuando un usuario real de AOL envía un email, pobox.com recive el email de un servidor de AOL.
2. Pobox controla el registro SPF de AOL, para asegurarse de que el servidor tiene permitido enviar emails de AOL.
3. El servidor se encuentra en la lista, así que Pobox deja **pasar** el mensaje.

Mensaje de un spammer.

1. Cuando un **spammer falsifica un mail** de AOL, Pobox recibe un mensaje de un servidor externo.
2. Pobox controla el registro SPF de AOL.
3. El servidor no está en la lista, así que Pobox **no deja pasar** al mensaje.

Registros SPF



Para trabajar con SPF se requieren dos cosas:

- **el servidor de correo desde el que se envía disponga de un registro TXT en el servidor DNS**.
- **que tanto el servidor de correo entrante como el saliente operen con SPF para saber cómo actuar**.

[8] http://spf.pobox.com

Veamos, un registro TXT en el servidor DNS:

"v=spf1 +a +mx +ptr include: ejemplo.net exp=spf-err ~all"

Y ésta es la explicación para cada uno de los parámetros de la línea de texto anterior:

v=spf1	Es el número de versión. Hay una.
a, mx, ptr y include	Son registros. Pueden existir uno o más registros.
+ y ~	Son prefijos. Los prefijos preceden a los registros -si no se especifican + se implica
exp	Es un modificador. Pueden ser cero, uno o dos modificadores.
all	Todas las IP, locales y remotas.
include	Dominios externos utilizados por los remitentes de e-mails locales, habituales cuando viajan.
a	Todas las IP del registro DNS A.
mx	Todos los registros A de cada registro host MX.
ptr	Todos los registros A de los registros host PTR.
ip4	Uno o más dominios especificados que utilizan Ip IPv4.
exists	Uno o más dominios especificados que se identifican como excepciones de las definiciones SPF.
+	La dirección ha superado el test. Ejemplo: +all
-	La dirección ha suspendido el test. Ejemplo: -all
~	La dirección ha suspendido el test pero el resultado no es definitivo. Ejemplo: ~all
?	La dirección no ha superado o ha suspendido el test. Ejemplo: ?all

Es fácil averiguar si un servidor de correo usa o no registro SPF en su servidor DNS. Para ello basta con abrir una ventana DOS y desde el indicador de comandos teclear:

nslookup -type=txt dominio.com

Veamos un ejemplo con un fabricante de servidores de correo que ya implementa SPF:

nslookup -type=txt altavista.com

Se invita a realizar la prueba para comprobar los resultados. Se apreciará una línea como la de más arriba, la entrecomillada con el registro TXT de ejemplo. Si se prueba con algún otro dominio, el resultado es probable que no incluya registro SPF.

Algunos nombres protegidos actualmente por SPF son:

- AOL.com
- Altavista.com
- DynDNS.org
- eOnline.com
- Earthlink.net
- Google.com
- GNU.org
- LiveJournal.com
- MotleyFool.com
- OReilly.com
- Oxford.ac.uk
- PairNIC.com
- Perl.org
- PhilZimmermann.com
- SAP.com
- Spamhaus.org
- Symantec.com
- Ticketmaster.com
- w3.org

La segunda parte implica activar SPF en el servidor de correo. Tomando como ejemplo al fabricante Alt-N y su servidor de correo MDaemon, la activación de SPF en uno de sus menús involucra examinar los encabezados SPF de todos los mensajes entrantes. Un encabezado típico sería:

Received-SPF: pass (ejemplo.mail: domain of pepe@altn.com
designates 65.240.66.16 as permitted sender)
x-spf-client=MDaemon.PRO.v7.1.0.R
receiver=ejemplo.net
client-ip=65.240.66.16
envelope-from=<pepe@altn.com>
helo=smtp.altn.com

Si este servidor de correo obtiene un error, bloquea el mensaje para siempre, cerrando la conexión y colocando al remitente en lista negra. Además, añade un filtro heurístico de correo basura, por el cual según provenga de un servidor con registro SPF en sus DNS o no, o de un servidor de correo preparado para SPF, adoptará unos condicionales de puntuación para SpamAssassin[9].

Una forma fácil de generar una entrada TXT para el servidor, es utilizar el asistente de este sitio:

http://spf.pobox.com/wizard.html

[9] Es un filtro de spam. Puede verse más información en: http://www.spamassassin.org/index.html

11. La ley CAN SPAM ACT

La ley **CAN SPAM ACT** del 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establece los requerimientos para aquellos que envían e-mails comerciales, dicta las penas para los spammers y las compañías que violan la ley (cuyos productos son promocionados mediante el spam), y otorga a los consumidores el derecho de solicitar no recibir más correo basura.

La ley, que entró en vigencia el 1 de enero de 2004, cubre el e-mail cuyo principal propósito es promocionar o promover un producto o servicio comercial, incluyendo contenido en un sitio Web. La ley se dirige contra los "correos basura" más insolentes: los de contenido pornográfico, los que ofertan todo tipo de remedios para mejorar la imagen física y, en tercer lugar, para hacerse millonario de golpe.

Lo que requiere la Ley

Para que estén de acuerdo con la Ley, los spammers tienen las siguientes restricciones:

- **Prohíbe información de cabecera de los e-mails falsa o engañosa**. La información de ruta de los e-mails, así como los campos “From” y “To”– incluyendo el nombre del dominio de origen y la dirección de e-mail – deben ser precisos y deben identificar a la persona que envía el e-mail. La medida prohíbe a los "spammers" o propagadores de "spam" esconderse detrás de identidades falsas o encabezamientos engañosos, bajo pena de multas de hasta un millón y medio de dólares y sentencias de cárcel de hasta cinco años.

- **Prohíbe “subjects” engañosos.** El asunto no debe engañar al receptor sobre los contenidos del mensaje.

- **Requiere ofrecer a los receptores un método para cancelar la recepción.** Los spammers deben proveer una dirección de correo de respuesta o algún otro tipo de mecanismo de respuesta basado en Internet que permita a los receptores comunicar que no desean recibir en el futuro más e-mails y los spammers deben respetar estos deseos.

- **Requiere que el e-mail comercial sea identificado como tal, y que incluya una dirección física postal verdadera.** La ley establece que indiquen su contenido con abreviaturas como **adv** (para publicidad) para que se puedan filtrar con facilidad.

Lista anti-spam

Además de la ley anti-spam, el senado estadounidense aprobó la creación de una lista que evitará recibir los e-mails. Esta medida podría permitir a los usuarios **inscribirse en una lista para no recibirlos**.

Este registro sería similar al que se creó en EEUU para la publicidad telefónica, que obliga a las compañías que realizan las fastidiosas llamadas a cualquier hora del día, incluso los fines de semana, a excluir los números que se han apuntado en la lista.

La **FTC** (Comisión Federal de Comercio en los EEUU), que tendrá que **encargarse de la creación de este registro** en un plazo de seis meses, habrá de encontrar una fórmula ingeniosa ya que, a diferencia de la lista de teléfonos, **la de direcciones de correo electrónico no se les facilitará a los "spammers", que podrían aprovecharla para acribillar a sus víctimas.**

Críticas sobre la Ley

- Actualmente existen leyes en 22 estados para perseguir el envío de correos comerciales no solicitados, pero no existe ninguna ley federal, lo que permite a los infractores escapar sin dificultad de las garras de las autoridades. Si resulta complicado hacer cumplir la Ley dentro de los EEUU, mucho más difícil sería hacerlo fuera.

  Para muchos críticos la medida está lejos de ser una panacea. Timothy Muris, el presidente de la FTC, anticipó que este registro no funcionará debido a las **dificultades para obligar a los "spammers", muchos de los cuales viven fuera de EEUU, a respetar estas restricciones.**

  Para peor, los spammers con sede en los Estados Unidos pueden trasladar su actividad al exterior, quedando así fuera de alcance para las leyes federales. Mientras exista otro país al que el spammer se pueda mudar, la cantidad de spam no va a disminuir.

- **Para otros críticos**, se trata de una legislación llena de agujeros por donde muchos "spammers" podrán colarse y continuar con su bombardeo inclemente. La ley prohíbe además a los individuos que emprendan acciones legales contra los "spammers". **Este privilegio queda reservado a los proveedores de correo,** como America Online, Microsoft o Yahoo.

- Las cláusulas de la Ley permiten que las empresas envíen mensajes de marketing siempre y cuando les brinden a los consumidores un mecanismo que les permita optar por ser eliminados de la lista de destinatarios para no recibir ese tipo de mensajes en el futuro (modalidad ésta conocida como "opt-out").

  Sin embargo, a la gente se le ha enseñado que no deben contestar a los mails de los spammers pidiendo ser borrados de la lista, a menos que quieran confirmar que su dirección de correo electrónico está activa. Entonces, en lugar de arriesgarse a confirmar sus direcciones a una empresa ilegítima, los consumidores simplemente van a bloquear todos los mensajes de remitentes desconocidos.

En definitiva lo que la Can-Spam en realidad está haciendo es crear una zona liberada para el spam, ya que legitimiza el spam en la gran mayoría de los casos.

La autenticación del correo electrónico ha sido aclamada por los tecnólogos como la única solución segura para el problema del spam. Sin este mecanismo, es probable que los usuarios de Internet queden indefensos ante la llegada de cantidades cada vez mayores de spam en los próximos años.

12. Noticias relacionadas

- *El proveedor brasileño UOL limita el envío de mensajes a 50 destinatarios*. La medida esta enfocada a reducir el spam. La medida esta siendo aplicadas a todos los clientes sin excepción.

Según explica en un mensaje la empresa, la medida se ha tomado para evitar el envío de spam desde cuentas de UOL y, cualquier usuario que remita un e-mail a más de 50 destinatarios, recibirá de inmediato un mensaje de error.

UOL es considerado como una de las fuentes emisoras más importantes de Spam desde Brasil y figura en las listas negras de distintas organizaciones que combaten el envío de mensajes no solicitados.

- *Un sitio Web publica el primer mapa del spam donde se muestran las relaciones entre las distintas empresas que lo practican.*[10]

Una organización: Clueless Mailers, revela por primera vez quiénes y cuántos conforman ese gran negocio que mueve centenares de millones de correos electrónicos y a los que nunca se les escapa ninguna nueva dirección de correo electrónico.

En un completo trabajo, Clueless Mailers ha elaborado un mapa en el que se aprecian, además, los vínculos entre esas empresas y cómo entre ellas se intercambian información, listas y clientes.

- *Una investigación realizada por WBI Brasil demostró que no siempre los mensajes comerciales no solicitados acaban en la papelera.*

"El usuario normal generalmente no tiene ninguna restricción contra los e-mails de propaganda, sean de marketing o spam. Si el asunto les interesa, leen el mensaje, como dijeron más de la mitad de los entrevistados. Solamente una cuarta parte de los usuarios borran el mensaje sin verificar su contenido", explica el coordinador de la investigación Paulo Roberto Kendzerski.

Este hecho provoca que un elevado número de usuarios haya adquirido algún tipo de producto tras recibir un mensaje comercial, aunque este haya sido recibido dentro de la categoría de spam. Lo que lleva a la conclusión de que no siempre este tipo de mensajes acaban en la papelera y que producen beneficios para las firmas que los emiten.

- *Evitar emisión del spam*

En una mesa redonda sobre el spam, realizada en Barcelona el pasado 09/07/2004, los tres panelistas, **Juan Carlos Plaza** (responsable de formación del Área de Nuevas Tecnologías de Broseta Abogados), **Manuel Medina (**Director General de es-Cret y Presidente de Inetsecur) y **Jacobo Crespo** (Territory Manager para España y Portugal de Sybari) coincidieron en la idea de acabar con el spam desde sus orígenes.

[10] http://www.cluelessmailers.org/spamdemic/mapfullsizegiflow.html

"Los proveedores de correo electrónico deberían aumentar la seguridad de sus servidores con herramientas que impidan la **emisión** de spam desde las direcciones de sus usuarios, en lugar de optar por medidas dirigidas al aumento del ancho de banda, ofrecido como solución para disminuir los colapsos y retrasos en las entregas, provocados por el incremento de volumen de tráfico debido al spam", afirma Manuel Medina de es-Cret.

La idea es implantar soluciones de detección de spam, y no de prevención.

La propagación del spam se beneficia de las cuentas de correo gratuitas, pues muchas de ellas no poseen protección alguna contra este tipo de ataques, y son el medio conductor perfecto para el "envío masivo de correos electrónicos y la propagación de virus troyanos".

- *AOL regaló entre sus abonados un Porsche confiscado a un spammer*

Efectivamente, AOL sorteó el porsche entre sus abonados, que había recibido como parte de la sentencia de un juicio que ganó al spammer. La Ley CAN SPAM ACT empieza a dar algunos frutos a pesar de todas las críticas. AOL es uno de los oponentes más ruidosos del spam y ha unido fuerzas con Microsoft, Yahoo y Earthlink para demandar a cientos de spammers.

- *Más leyes anti-spam*

Muchos países han empezado a defenderse de los ataques de spammers mediante legislaciones. Entre ellos están Colombia, Argentina, Macedonia, Italia, Australia, UK, Canadá, entre otros. Mayor información puede obtenerse en:

http://research.yale.edu/lawmeme/spam.php.

- *Herramientas anti-spam disponibles.*

Para protegerse de la presión del spam y sacar a flote el buzón de correo, se puede utilizar cualquiera de las siguientes herramientas.

S.O.	Herramienta	Dirección
Windows	MailWasher	http://www.mailwasher.net/
	K9 AntiSpam	http://keir.net/k9.htm
	Email Control	http://www.abreuretto.com/anti-spam/indexi.htm
	Mailboxfilter	http://www.mailboxfilter.com/
Linux	MailScanner	http://www.sng.ecs.soton.ac.uk/mailscanner
	Active Spam Killer	http://www.paganini.net/ask
	SpamAssasin	http://spamassassin.org/
Mac	Spamnix	http://www.spamnix.com/
	Spamfire	http://www.matterform.com/

Apéndice A – Información extraída del sitio de Paul Graham

A continuación presento un esquema de cómo realizo el filtrado estadístico. Comienzo con un grupo de correo que es spam y uno que no lo es. En el momento cada uno de ellos contiene cerca de 4000 mensajes. Exploro todo el texto, incluyendo las cabeceras y código html o javascript embebido, de cada mensaje en cada grupo. Por ahora considero los caracteres alfanuméricos, rayas horizontales, apóstrofes y signos de dólar como parte de lexemas, y todo lo demás como separadores de lexemas. (Probablemente hay espacio para introducir mejoras aquí.) Ignoro todos los lexemas que son formados completamente por dígitos, e ignoro también los comentarios html; no los considero siquiera como separadores.

Cuento el número de veces que cada lexema (sin diferenciar mayúsculas de minúsculas, por el momento) aparece en cada grupo. En este punto resulto con dos grandes tablas asociativas, una para cada grupo, que contienen referencias de los lexemas hacia el número de ocurrencias de cada uno.

A continuación creo una tercera tabla asociativa, esta vez creando referencias para cada lexema hacia la probabilidad de que un correo electrónico que lo contenga sea spam, la cual calculo de la siguiente forma:

```
(let ((g (* 2 (or (gethash word good) 0)))
      (b (or (gethash word bad) 0)))
  (unless (< (+ g b) 5)
    (max .01
         (min .99 (float (/ (min 1 (/ b nbad))
                            (+ (min 1 (/ g ngood))
                               (min 1 (/ b nbad)))))))))
```

en donde `word` es el lexema cuya probabilidad estamos calculando, `good` y `bad` son las tablas asociativas que he creado en el primer paso, y `ngood` y `nbad` son el número de mensajes de no-spam y spam respectivamente.

He explicado esto mediante código para mostrar un par de detalles importantes. He querido cargar las probabilidades ligeramente para evitar los reportes falsos, y por ensayo y error he encontrado que una buena forma de hacerlo es doblando todos los números en `good`. Esto ayuda a distinguir entre palabras que ocurren ocasionalmente en correos electrónicos legítimos y las palabras que casi nunca lo hacen. Únicamente considero las palabras que ocurren más de cinco veces en total (en realidad, y debido al doblado de valores, una ocurrencia de tres veces en el correo no-spam sería suficiente). Y luego está la pregunta sobre qué probabilidad asignarle a las palabras que ocurren en un grupo pero no en el otro. De nuevo por ensayo y error he elegido 0.01 y 0.99. Puede haber campo para realizar ajustes aquí, pero a medida que los grupos crezcan estos ajustes ocurrirán automáticamente después de todo.

Aquellos especialmente observadores notarán que aunque considero cada grupo como un solo flujo de texo para el propósito de contar ocurrencias, uso el número de correos electrónicos en cada uno, en lugar de su longitud combinada, como el divisor al calcular las probabilidades de spam. Esto añade otra pequeña recarga para protegernos de los reportes falsos.
Cuando llega correo nuevo, es analizado y descompuesto en lexemas, y los quince más interesantes, en donde el nivel de interés se mide por qué tan lejos se encuentra su probabilidad de spam de un neutral 0.5, son usados para calcular la probabilidad de que el correo sea spam. Si `probs` es una lista de las quince probabilidades individuales, la probabilidad combinada se calcula entonces como:

```
(let ((prod (apply #'* probs)))
  (/ prod (+ prod (apply #'* (mapcar #'(lambda (x) (- 1 x))
                                     probs)))))
```

Una pregunta que surge en la práctica es qué probabilidad asignarle a una palabra que nunca ha visto, es decir, una que no aparece en la tabla asociativa de probabilidades de palabras. He encontrado, nuevamente por ensayo y error, que 0.4 es un buen número para utilizar. Si nunca ha visto cierta palabra antes, probablemente haya un buen chance de que sea inocente; las palabras incluidas en el spam tienden a ser demasiado familiares.

Hay ejemplos de la puesta en práctica de este algoritmo sobre correos electrónicos reales en uno de los apéndices al final de este documento.

Considero un correo como spam si el algoritmo descrito anteriormente le da una probabilidad de más de 0.9 de ser spam. Pero en la práctica no importaría mucho en dónde coloco este límite, ya que muy pocas probabilidades terminan en la mitad del rango.

Ejemplos de cómo aplicar esta técnica pueden verse en **http://www.paulgraham.com**

Apéndice B – Información proveída por los compañeros

Open Relay

Un Open Relay consiste en que un servidor de correo procese un mensaje de correo en el que el remitente y el destinatario son usuarios que no forman parte del dominio local.

Por ejemplo: un usuario conectado al servidor1 desea enviar un correo a otro usuario conectado al servidor2, pero utilizando su cuenta de correo existente en un servidor3, si esta operación puede ser realizada con éxito se dice que el servidor3 es un servidor *Open Relay* y cualquier usuario del mundo puede enviar un mail a través de él.

Cada servidor que permite a usuarios no autorizados el envío de correo, tarde o temprano cae en manos de los spammers, lo que puede acarrear consecuencias muy serias.

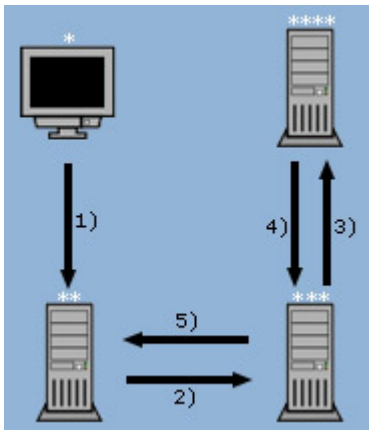
- Primero: porque puede provocar una reducción de eficacia del servidor, el cual en vez de recibir y entregar mensajes a usuarios autorizados, enviará spam. Esto se conoce como secuestro de servidor, mediante el cual se enrutan enormes cantidades de correo por el mismo.
- Segundo: La dirección IP del servidor terminará en las listas negras y muchos servidores dejarán de recibir sus mensajes (la eliminación de la IP de muchas listas negras es muy difícil, incluso a veces imposible).

Internet se encuentra llena de Open Relay, muchos de ellos lo son por estar mal configurados y no tener una correcta autentificación de usuarios.

Entre las listas negras más utilizadas se encuentra SpamCop.net, que se maneja en base a donaciones, y por el lado de las bases de datos de servidores Open Relay, podemos encontrar ORDB: ORG, o Relay Stop List, de Visi.com, etc.

¿Cómo trabaja el ORDB?

Se explicará con relación al grafico siguiente donde: * es el usuario, ** servidor de correo saliente, *** servidor de correo de mensaje entrante del receptor, **** servidor ORDB.



1. El usuario envía un correo al servidor de correo saliente (Servidor SMTP).
2. El servidor de correo saliente establece una conexión con el servidor de correo del receptor e intenta enviarle el correo.
3. El servidor de correo del receptor consulta la base de datos ORDB para verificar si el servidor de correo saliente pertenece a la lista de servidores Open Relay.
4. El servidor ORDB responde al servidor de correo receptor y le informa si el servidor de correo saliente pertenece o no a la lista.
5. Si el servidor de correo saliente no pertenece a la lista, el servidor de correo receptor puede elegir entre rechazar la conexión desde el servidor de correo saliente e informarle que no esta habilitado para enviar el correo o aceptarlo sin ningún problema.
6. El usuario entonces recibe una notificación llamada “bounce” o “Mailer Daemon” informando que el correo no pudo ser enviado.

Listas negras

¿Qué son las listas negras?

Con el tiempo han ido apareciendo diferentes iniciativas cuyos mecanismos intentan paliar la entrada de SPAM en los buzones de los usuarios. Estas iniciativas son lo que se llama listas negras de SPAM.

Las listas negras de DNS son listas de dominios e IPs que originan correo SPAM.

Cualquier empresa, institución o persona, que disponga de un servidor que permita el envío de correo basura, será incluido en una de las múltiples listas negras. Todas tiene el mismo fundamento: generar una base de datos de servidores de correo que están mal configurados y han sido o serán fuentes de SPAM.

Gran parte del software anti-SPAM utilizado por corporaciones e ISPs, usan estas listas para controlar el SPAM, rechazando cualquier email que se haya originado en uno de esos dominios o IPs. Algunas de esas listas son:

- **RBL** -Realtime Blackhole List- (MAPS-Mail Abuse Prevention System)
- **RSS** -Relay Spam Stopper - (MAPS)
- **DUL** -Dial-up User List-(MAPS)
- **ORDB** -Open Relay Data Base
- **ORBL** -Open Relay Black List
- **ORBZ** -Open Relay Blackhole Zones
- **MAPS** - http://www.mail-abuse.com/
- **Spam Cop** - http://www.spamcop.net/
- **SpamHaus** - http://www.spamhaus.org/
- **SPEWS.org** - http://www.spews.org/
- **ORDB.org** - Open Relay Database - http://www.ordb.org/

Las listas negras de DSN son mantenidas por organizaciones anti-SPAM, las cuales no son responsables del rechazo del correo, ya que no pasa por sus máquinas.

Una alternativa: las listas blancas

Muchas corporaciones e ISPs crearán lo que se llama Lista Blanca, que reúne direcciones IP que estas organizaciones creen seguras, ya que no envían SPAM a sus usuarios. Si un IP está incluido en una Lista Blanca, los e-mails que provengan de él no serán rechazados. Es por eso que es importante para empresas de Marketing respetables, trabajar con los ISPs más importantes del mercado, como por ejemplo **AOL**, ya que así se aseguran de figurar en su Lista Blanca, y que su correo de propaganda sea aceptado y enviado a los usuarios del ISP.

¿Cómo se ingresa a las Listas Negras?

Las listas negras guardan direcciones IP a partir de las denuncias de los usuarios que han sido víctimas de un SPAM. Cuando un usuario recibe un mensaje no solicitado, lo envía a uno de los organismos que controlan las Listas Negras y ellos, después de analizar sus cabeceras, determinan el servidor que lo ha enviado y si no es seguro, lo incluyen. Pero esto también facilita que uno sea incluido maliciosamente a través de una queja de un cliente o un competidor.

Muchas Listas Negras listan no solo el IP sospechado de enviar SPAM, sino también cualquier IP en ese rango de direcciones. Por ejemplo, si un usuario de un proveedor de Internet específico es acusado de realizar *spamming*, no solo él será incluido en la Lista Negra sino también los otros

usuarios. A veces, estos reciben notificaciones en los mails que son rechazados por algunos servidores por ser considerados SPAM, pero normalmente los usuarios no saben interpretar las notificaciones.

Para saber si un IP ha sido introducido, se puede ingresar a los sitios Web de la mayoría de las Listas Negras o softwares que las utilizan, ya que estos permiten introducir un número de IP para informar si este se encuentra en una determinada lista. Pero debido a la gran cantidad de listas existentes, es difícil asegurarse de no estar incluido en todas, ya que los software especializados realizan la búsqueda en determinadas listas, pero no en todas.

Otra manera de saber si el IP de un servidor está listado, es revisar el archivo .log del servidor, en el cual se encontrarán informes de rechazo debido a la inclusión del servidor en una lista.

Como algunos software filtran los emails sospechados de ser SPAM, ese filtrado puede dar lugar a la pérdida de mail legítimo de interés para una organización, encontrando lo que se llama Falso Positivo, (FP: false positives) o mails catalogados como SPAM pero que no lo son. Los FP reducen la eficiencia de la solución anti-SPAM.

¿Cómo salir de las Listas Negras?

Para proteger un servidor, se le debe realizar una configuración anti-relaying, de modo que no actúe como servidor de correo abierto.

Una vez que se está seguro que un servidor ya no permite hacer *Relaying*, se debe ingresar a las Listas Negras de servidores públicos para que lo den de baja. En algunos casos se debe seguir las instrucciones de los correos de los usuarios que han "rebotado", en las que se explica a que lista han sido adheridos.

En general, se debe ingresar a los sitios Web que proporcionan el servicio e introducir el número de IP deseado. Si se comprueba que el servidor ya no es un relé abierto, se lo da de baja de las listas manejadas por ese sistema.

- Uno de estos sistemas es el de **abuse.net**.[11]
- Otro sistema conocido es el **ORDB**.[12] Aquí puede tomar hasta 72 horas antes de que la solicitud sea atendida y que el IP sea eliminado de las Listas.
- Otra herramienta es el **Black List Monitor**[13], que chequea automáticamente el IP de la máquina comparándolo con las Listas, monitoreando constantemente si el estado del IP sufrió algún cambio, si fue enlistado o dado de baja.
- Otro sistema es el **spamcop.net**[14]. Una vez que se haya detenido el SPAM y cerrado el relay, el IP será dado de baja como máximo 48 horas después del último reporte de SPAM contra ese servidor. Si se ha cerrado el relay recientemente, se puede chequear si aún está registrado en ORDB. Si es así, se solicita su exclusión, y cuando es certificado como seguro, se ingresa de nuevo a spamcop.net para pedir la remoción, o se espera las 48 horas para que esta se realice automáticamente.

[11]) http://www.abuse.net/relay.html
[12]) http://www.ordb.org/removal/
[13]) http://www.blacklistmonitor.com
[14]) http://spamcop.net/bl.shtml

Leyes anti-spam en el mundo

Actualmente son varios los países que están promulgando leyes anti-spam en un intento por detener el la gran cantidad de correo no deseado que son recibidos por los usuarios de correo electrónico. A continuación se presentan los países que combaten de manera legal el spam junto con las medidas tomadas para tal propósito.

Argentina
No existe una ley específica en contra del spam, sin embargo, la Ley de Protección de Datos Personales (o Hábeas Data) regula, entre otras cuestiones, los archivos o bancos de datos con fines de publicidad y les da dos derechos a las personas que están registradas en esos bancos de datos:

1. Derecho a acceder sin cargo a la información que tengan sobre uno.
2. El titular podrá solicitar el retiro o bloqueo de su nombre de la base de datos.

Esta resolución reconoce que la dirección electrónica de una persona es un dato personal que merece protección y ha sido utilizada en acciones judiciales en contra de personas que venden bases de datos con direcciones de correo electrónica de miles de personas.

Canadá
Cuenta actualmente con 3 leyes anti-spam, sin embargo la cantidad de correo no deseado no ha disminuido. Por tanto, el gobierno estableció un grupo especial denominado “Special Task Force on Spam” el cual se encarga, entre otras cosas, de ver la manera reforzar las leyes existentes y la posibilidad de crear nuevas leyes anti-spam. Las leyes existentes son:

Personal Information Protection and Electronic Documents Act: Esta ley establece que las direcciones de e-mail pueden solo ser usados para los propósitos que son solicitados, y que los dueños de estas direcciones de e-mail deben consentir cualquier uso secundario.
Criminal Code: Contiene provisiones específicas que lidia con contenidos engañosos utilizados en los correos electrónicos.
Competition Act: Penaliza las acciones utilizadas para acceder sin autorización a sistemas de computadoras, tales como el uso de troyanos que es utilizada para reenviar el spam.

Japón
En Japón actualmente se está estudiando un proyecto de ley para combatir, en todo el país, los correos electrónicos no deseados. El proyecto de ley consta de 3 partes:

1. Los transmisores están obligados a advertir que el e-mail es una publicidad.
2. No se puede enviar correo electrónico publicitario a personas que manifestaron .que no desean recibirlos.
3. Las empresas de telecomunicación pueden rechazar correos electrónicos de spammers, si esto puede causar problemas.

España
La Ley sobre la Sociedad de la Información y el Comercio Electrónico fue promulgada en Octubre del 2000. Una versión posterior fue publicada en Enero del 2001 en la cual se establece que las personas dedicadas al envío de correo electrónico no solicitado deben consultar, al menos una vez al mes, o mantener ellas mismas las listas en las cuales aparecen las direcciones de correo electrónico de las personas que no desean recibir ese tipo de correo. Pueden consultar listas adicionales y además la palabra “Publicidad” o “Publi” debe ser colocada como asunto (subject) en los correos electrónicos no solicitados que son enviados.

La versión final de esta ley incluye provisiones que prohíben completamente el envío de correo electrónico no solicitado.

Italia

En Italia existen 3 leyes diferentes que defienden a los usuarios de Internet del spam:
DL 675/1996 Sobre protección privada: establece que una compañía debe contar con una autorización de la persona cuyos datos personales (como el email) desea utilizar.
DL 171/1998 sobre protección en las telecomunicaciones: establece que toda publicidad debe ser pagada por la empresa y no por el usuario (faxes y emails son también pagados por el usuario).
DL 185/1999 sobre la protección de los consumidores en contratos de larga distancia: establece que si una compañía desea vender algo fuera de un edificio comercial, para publicitar sus productos debe contar con autorización del usuario.

Dinamarca
A partir de Junio del 2000 el spam ha sido prohibido mediante el Marketing Practices Act. Posteriormente se realizó una enmienda a la sección 6a de esta ley, la cual establece una excepción a la prohibición. Si el consumidor, mediante alguna compra, ha proporcionada su dirección de correo electrónico a alguna compañía, ésta tiene permitido enviar spam a la dirección proporcionada por el consumidor.

Austria
El Artículo 101 de la Ley Federal establece que el envío de correo electrónico en masa o para propósitos de publicidad debe contar con el consentimiento previo del receptor del correo.

Yugoslavia
La Iniciativa Yugoslava Anti-Spam (YASI) provee una explicación completa de todos los tipos de abusos en la red, medidas preventivas, medidas de protección, etc. Sin embargo no existe una ley específica que prohíba el spam.

Bélgica
La ley belga establece lo siguiente en cuanto a la publicidad mediante correo electrónico:
Cuando se realiza publicidad mediante correo electrónico, el transmisor debe asegurarse de proveer información clara y comprensible referente al derecho de rechazar tal publicidad en el futuro. La ley prohíbe estrictamente la utilización de direcciones o identidades de terceros y la falsificación de información que hace posible identificar el origen del mensaje.

Finlandia
La ley finlandesa prohíbe el envío no solicitado de publicidad a personas y grupos de noticias. Establece que toda comunicación a través de Internet es confidencial.

Francia
No existen leyes específicas Sin embargo con las leyes existentes se pueden condenar ciertas acciones llevadas a cabo por los spammers. Ya que si el transmisor daña algún servidor o perjudica a alguna compañía de alguna manera mediante spam, se lo puede demandar sin importar que el daño haya sido o no realizado de manera conciente.

Grecia
De acuerdo a la información que posee la comisión europea, Grecia a promulgado una ley que requiere previo consentimiento de los receptores de sistemas automáticos de llamadas, faxes y e-mails.

Irlanda
No existen leyes específicas relativas al spamming. La acción del gobierno se limita a instar el desarrollo de códigos de práctica que deben ser seguidos por personas que realizan comunicación comercial no solicitada mediante e-mail.

Otros países que cuentan con legislación anti-spam son los siguientes: Luxemburgo, Países Bajos, Noruega, Portugal, Suecia, Reino Unido.

Software Anti-Spam

McAfee → SpamKiller

- Bloquea e-mails usando las listas y prefija los filtros
- Puede filtrarse MSN/Hotmail, POP3 y e-mail de MAPI
- Puede personalizarse filtros
- Cuarentena de e-mails spam
- Lista segura de amigos

Casos judiciales contra Spammers

Estos artículos se refieren a los casos judiciales y demandas que vienen realizando las grandes empresas de ISP y correo electrónico contra los spammers.

Muchas de estas compañías ya habían presentado demandas en años anteriores contra las empresas y personas responsables de ese tipo de mensajes, basándose en leyes estatales, en los estados de Florida, California, Georgia, Virginia, Washington y otros, obteniendo algunas confiscaciones de propiedades, bienes de los spammers, fuertes multas y castigos como la prohibición de enviar mensajes comerciales por cierto tiempo.

Con la nueva ley, la ley federal llamada CAN-SPAM que entró en vigor el 1 de enero de este año se espera que la lucha contra la práctica del spam sea mas efectiva y sobre todo que se impongan penas mayores.

A continuación se presentan algunos artículos publicados con referencia a la lucha anti-spam de las grandes compañías y en la parte de *Anexo* se presentan los casos y demandas específicas de cada compañía para las personas que estén interesadas en saber.

AOL (grupo Times Warner), Microsoft, Yahoo y Earthlink presentan demandas contra "spammers"

Los principales proveedores americanos de acceso a internet AOL, Microsoft, Yahoo y Earthlink, han anunciado su primera ofensiva judicial común contra los emisarios de correos no deseados, 'spam', desde la entrada en vigor de una nueva ley federal sobre el tema bautizado como 'Can-Spam Act'
Los cuatro mayores proveedores de servicios de Internet (ISP) y correo electrónico de Estados Unidos anunciaron en una conferencia de prensa conjunta celebrada en Washington, la presentación de seis pleitos contra cientos de demandados, entre los que figuran algunos de los más conocidos emisores de correos electrónicos comerciales no solicitados.
Cada una de las cuatro compañías presentó denuncias ante cortes federales de California, Georgia, Virginia y el estado de Washington. Microsoft, Yahoo!, AOL y Earthlink acusan a los demandados de haber mandado en total cientos de millones de 'spam' a usuarios de sus cuatro redes.
La nueva ley, sin prohibir los correos no deseados, autoriza a los usuarios de internet a reclamar su retirada de las listas de difusión y castiga a los que envían mensajes engañosos o con carácter pornográfico sin advertir previamente a los que los reciben.
Varias encuestan han afirmado que los correos no deseados representan hoy en EEUU la mitad o más del volumen de tráfico de e-mails y cuesta cada vez más a las empresas en pérdida de productividad o en equipos informáticos de filtrado.
En las quejas presentadas se reprocha a los 'spammers' sus artimañas para captar a los internautas, prometiendo dinero rápido e incluso diplomas universitarios. También se les acusa de tomar prestadas identidades falsas para esquivar más fácilmente los filtros.

Cuatro individuos acusados en EEUU por enviar correo basura

Las autoridades anunciaron aquí que han presentado las primeras cuatro acusaciones penales de conformidad con una legislación reciente contra el llamado correo basura electrónico, conocido en inglés como "junk mail" o "spam".

Documentos jurídicos presentados en un caso decisivo en Detroit describen una madeja casi inescrutable de identidades corporativas, cuentas bancarias y empresas electrónicas virtualmente inexistentes en una sola operación para ese tipo de correo, según informó AP.

En uno de los casos, según los investigadores, ciertos paquetes eran entregados en un restaurante, donde un individuo los recibía y los entregaba a uno de los cuatro acusados.
Funcionarios de la Comisión Federal de Comercio que se disponían a anunciar los arrestos el jueves, dijeron a investigadores postales que habían recibido más de 10 mil quejas acerca de correo electrónico basura enviado por los acusados.
Los documentos judiciales identificaron a los acusados como Daniel J. Lin, James J. Lin, Mark M. Sadek y Christopher Chung, todos de West Bloomfield, Michigan, cerca de Detroit.
Los individuos fueron acusados de ocultar sus identidades en cientos de millares de avisos electrónicos destinados a promover productos fraudulentos para bajar de peso y de enviar su correo basura rebotándolo a través de computadoras que carecían de protección contra el "spam".
Chung y Sadek se presentaron ante un tribunal federal de distrito y fueron dejados en libertad bajo fianza sin garantía, dijo Gina Balaya, portavoz de la Fiscalía Federal.
Agregó que los dos acusados de apellido Lin no han sido detenidos.
El abogado de Sadek, James L. Feiberg, dijo que los agentes federales llegaron a la residencia de Sadek en las primeras horas de la mañana "cuando menos se los esperaba" y lo arrestaron.
Jueves, 29 abril 2004
IBLNEWS, AGENCIAS

Lucha legal de AOL contra el correo electrónico no deseado

AOL ha establecido un largo y exitoso récord cuando se trata de litigar contra remitentes de correo electrónico no deseado (spammers). Desde 1996, AOL presentó 28 demandas contra más de 200 individuos y corporaciones donde se les acusaba de enviar correo electrónico no deseado a sus suscriptores. Como resultado de estos esfuerzos legales proactivos para ayudar a proteger a sus suscriptores contra el correo no deseado, AOL ganó mandatos de la Corte para detener a los remitentes de dicho correo, ganó millones de dólares por daños y perjuicios, y mandó a los remitentes de correo no deseado a bancarrota.
Más recientemente, AOL se unió a sus socios de la industria Microsoft, Earthlink y Yahoo! para dar a conocer las primeras y más importantes demandas civiles de la industria contra cientos de remitentes de correo no deseado por medio del uso de la nueva ley federal CAN-SPAM. AOL también presentó una demanda civil en febrero ante la Corte Federal de Florida contra cuatro acusados, denominados los “Remitentes de Correo no Deseado del Estado del Sol” ("Sunshine State Spammers"), los cuales realizaron conspiraciones con operadores internacionales de correo no deseado en Tailandia para enviar correo no deseado a la red de AOL.
En diciembre, AOL colaboró con el Fiscal de Virginia Jerry Kilgore y otros para dar a conocer las primeras cinco acusaciones bajo el nuevo estatuto de Virginia contra el correo electrónico no deseado, el cual es el más riguroso del país. Los remitentes de correo electrónico no deseado de Carolina del Norte están acusados por enviar spam los suscriptores de AOL y podrían enfrentarse a la cárcel, a la confiscación de bienes y a multas de dinero.

Pueden Ser Condenados a cinco años de cárcel.
(26-08-04) Estados Unidos redobla su batalla contra el correo basura realizando arrestos masivos de "spammers"

LD (EFE) Los arrestos, que podrían ser anunciados este jueves en Washington por el fiscal General, John Ashcroft, incluyen también a acusados de realizar otros delitos, como el robo de identidad o de fraudes con tarjetas de crédito. Esta operación sería la mayor para este tipo de delitos y la más importante desde que se aprobó en diciembre pasado la nueva ley que sanciona a quienes envían mensajes electrónicos basura que buscan engañar a los usuarios de Internet.
Quienes sean encontrados culpables de estos delitos se enfrentan a penas de hasta cinco años de cárcel.
Agentes federales, ejecutivos y expertos de la industria informática formaron un equipo que ha obtenido una importante base de datos de quienes envían este tipo de correo basura. En algunos

casos, el grupo adquirió productos promocionados para dar con la verdadera identidad de quienes estaban detrás de estas operaciones.
El periódico explica que algunos expertos creen que operaciones como ésta podrían disuadir a quienes siguen operando en el negocio ilícito de enviar correo basura. Pero otros creen que esto sólo hará que el problema se traslade fuera de EEUU, y que operadores en países como Rusia coparían el mercado dejado libre por los programadores estadounidenses.

California multa a spammers con US$2,000,000

PW Marketing es la primera empresa castigada fuertemente por envío masivo de correo no solicitado y otras prácticas de spamming.
Un tribunal californario impuso la multa de dos millones de dólares a consecuencia del envío masivo de emails sin consentimiento del destinatario. Estos emails no solo enviaban publicidad, sino que daban indicaciones para ser reenviados y crear una cadena aun mayor, sin indicar procedente que permitiera rastrear al responsable. La empresa no solo tendrá que pagar la multa sino que no podrán realizar publicidad en internet en los próximos 10 años.
Los fiscales se basaron en una ley sancionada en 1998 que regula esta dañina práctica y que menciona que cualquier individuo puede demandar a empresas que envíen spam hasta por un valor de mil dólares por mensaje enviado que no tenga permiso de recepción de parte del destinatario.
Fuente: Agencias/Vnunet

Microsoft Corp. vs. John Does 1--50, negocios como Super Viagra Group (U.S. District Court, Western District of Washington)
Esta demanda sostiene que Super Viagra Group ha enviado cientos de millones de mensajes de correo electrónico ilegales a suscriptores de Microsoft Hotmail anunciando ya sea "Super Viagra" o un parche para pérdida de peso. Las prácticas de correo electrónico de este grupo de correo no deseado (spam) son sofisticadas y violan al Ley CAN-SPAM federal y otras leyes estatales y federales.
La demanda contiende que Super Viagra Group envía sus mensajes de correo electrónico a través de proxies abiertos y computadoras secuestradas en países alrededor del mundo, utiliza información de transmisión y líneas de asunto engañosas, y toma medidas para disfrazar la identidad de los remitentes. La demanda identifica casi 40 nombres de dominio a través de los cuales se pueden adquirir, supuestamente, productos de Super Viagra Group. Los dominios identificados están registrados a nombre de individuos en Argentina, Corea del Sur, India, Lituania, Rusia, Sudáfrica y Turquía.

Supuestas violaciones a CAN-SPAM

- Proxies abiertos para algunos o todos los mensajes de correo electrónico
- Direcciones falsas de remitente en todos o casi todos los mensajes de correo electrónico
- Líneas de asunto engañosas en algunos mensajes de correo electrónico
- Falta de dirección física en la mayoría de los mensajes de correo electrónico
- Omisión de la opción electrónica de cancelación de suscripción en algunos mensajes de correo electrónico

Bibliografía

Introducción e historia del spam
http://es.wikipedia.org/w/wiki.phtml?title=Spam&amp
http://alerta-antivirus.red.es/
http://www.seguridadenlared.org/amenazas/spam/default.htm
http://www.laflecha.net/canales/seguridad/200407092/
http://www.zonagratuita.com/servicios/noticias/2004/abril/spam3.htm

Técnicas AntiSpam
http://www.argo.es/%7Ejcea/antispam/
http://kapcoweb.com/p/static/docs/un-plan-para-el-spam/un-plan-para-el-spam.html
http://www.paulgraham.com/antispam.html

Ley Can Spam Act
http://www.noticiasdot.com/publicaciones/2003/1003/2410/noticias241003/noticias241003-5.htm

SPF
http://spf.pobox.com/
http://www.seguridad0.com/index.php?ID=592

Otros
http://www.rzweb.com.ar/modules.php?name=News&file=article&sid=1581
http://www.argo.es/%7Ejcea/antispam/noticias.htm
http://www.zonavirus.com/Detalle_ARTICULO.asp?ARTICULO=126

3. Índice