

Introducción

Se denomina correo basura (en inglés también conocido como junk-mail o spam) a una cierta forma de inundar la Internet con muchas copias (incluso millones) del mismo mensaje, en un intento por alcanzar a gente que de otra forma nunca accedería a recibirlo y menos a leerlo. La mayor parte del correo basura está constituido por anuncios comerciales, normalmente de productos dudosos, métodos para hacerse rico o servicios en la frontera de la legalidad. No deja de amargar la existencia a los usuarios de Internet cuando encuentran sus buzones rebosando con correos del estilo

Qué es el Spam

Originalmente 'Spam' se llamo al jamón con especias (Spiced Ham) producido por *Hormel* en 1926 como el primer producto de carne enlatada que no requería refrigeración. Esta característica hacia que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial. Tal vez por esto se ha utilizado el término para calificar el correo electrónico no solicitado, y se ha convertido en una de las mayores molestias para las personas en la red.

'Spam' entonces es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a la Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector. Contrario al 'correo basura' o *Junk Mail* que recibimos en nuestros buzones ordinarios (físicos, en papel!), el recibo de correo por la red le cuesta a un buen numero de personas, tanto en la conexión como en el uso de la red misma. El correo físico no tiene ningún costo para quien lo recibe.

Inicialmente Internet no permitía su uso comercial, pero ya se ha comprobado que el uso comercial es el que sostiene su infraestructura. Por lo tanto, la definición en ese entonces se refería exclusivamente a "correo no solicitado" y tenia implícito que no era comercial. Hoy con el uso comercial, este correo no solicitado se puede separar en el *comercial*, o sea el que quiere venderle algo, y el *informativo*, que le informa de un evento u ofrecimiento que no implica una erogación económica para el receptor.

La clasificación del Spam

Para obtener una clasificación precisa y certera de los mensajes, se

Requiere un cierto "entrenamiento" del sistema. Ese entrenamiento ya ha

Sido realizado, pero es necesario mantenerlo "fresco" para asegurar la

Calidad del sistema.

En general el personal técnico de Argo está buscando:

- a) Mensajes "buenos" con una probabilidad de SPAM superior al 20%.
- b) Mensajes "SPAM" con una probabilidad de SPAM inferior al 95%.

Si dispone de ejemplos de mensajes con estas características, puede

Hacémoslos llegar a la dirección "jcea@argo.es", con el tema "mensaje a

Reclasificar". Es tremendamente importante que nos haga llegar el Mensaje problemático inalterado, tal cual le haya llegado a su buzón. En El Microsoft Outlook, por ejemplo, DEBE usar la opción de "reenviar Como adjunto".

ESTADÍSTICAS:

Aproximadamente el 40% de los mensajes que recibe ARGO son SPAM, lo que Supone un coste apreciable en ancho de banda y capacidad de disco duro Para almacenar los buzones de nuestros usuarios.

De los mensajes identificados como SPAM, el 50% está siendo filtrado ya en el servidor de correo, ya que se trata de destinatarios que ya han seleccionado el "nivel avanzado" de filtrado.

Tipos más comunes

Spam: enviado a través del correo electrónico.

Spim: específico para aplicaciones de tipo Mensajería Instantánea (MSN Messenger, Yahoo Messenger, etc).

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

Spam SMS: *spam* destinado a enviarse a dispositivos móviles mediante SMS (Short Message Service).

Otros tipos más comunes de spam

En todo el mundo, el spam tiende a anunciar cierta gama de bienes y servicios, sin que importe el lenguaje y la geografía. En adición, el spam cambia según la estación del año, por ejemplo en Navidad; o cuando en los anuncios de calefactores son reemplazados en verano por sistemas de aire acondicionado.

Sin embargo, en el transcurso del año, el 50% del spam pertenece a las siguientes categorías:

Pornografía

Salud

Tecnologías informáticas

Finanzas personales

Educación/entrenamiento

Pornografía

Esta categoría incluye ofertas de productos diseñados para aumentar o mejorar la potencia sexual, enlaces a sitios pornográficos o anuncios de pornografía, etc. Por ejemplo (por razones éticas incluimos sólo texto y no gráficos):

Tema: Una ayuda muy barata para su erección :-)
¡Buenos días!
¡Le ofrecemos la Viagra más barata del mundo!
La puede comprar en: {ENLACE}
Sinceramente, Liza Stokes

Tema: Tema: Creo que te gustará ver cómo me corro :-)
Hola...soy Brooke...y acabo de conseguir una cámara web...charlemos un poco...mientras me pongo guarra...ja, ja ;-)
{ENLACE}

Salud y medicina

Esta categoría incluye anuncios de sistemas para adelgazar, para el cuidado de la piel, el mejoramiento de la postura, la cura de la calvicie, suplementos de dietas, medicina no tradicional, etc. que pueden ser comprados en línea.

Ejemplos:

Tema: Pierda hasta el 19% de su peso. Un nuevo sistema para adelgazar está aquí.
Hola, tengo una oferta especial para tí...
¿QUIERES PERDER PESO?
El sistema más poderoso de pérdida de peso ahora está disponible sin prescripción médica. Completamente natural: Adipren720 ¡100% de garantía, o te devolvemos el dinero!
– Pierde hasta el 19% del peso de su cuerpo. – Más del 300% de pérdida de peso si estás haciendo dieta. – Pierde el 20–35% de grasa abdominal. – Reducción del 40–70% de grasa subcutánea. – Aumenta tu metabolismo en un 76,9% sin hacer ejercicios. – Quema las grasas calorizadas. – Quita las ganas de consumir azúcar. – Aumenta la confianza en tí mismo y la autoestima.
Más detalles sobre Adipren720: {ENLACE}

Tema: Precios bajos legales para Valium (Diazepam) (SIN cafeína)
El Servicio de Ventas Rx te ofrece nuestro último producto:

Un servicio personal de compras que provee legalmente
drogas sin prescripción médica desde Canadá y el resto del mundo.

Haz tu pedido de Valium (Diazepam) y te garantizamos que lo tendrás en tu casa en 7
DÍAS.

No te pierdas nuestra Cantidad Limitada*

Visítanos aquí: {ENLACE}

Tecnologías informáticas

Esta categoría incluye ofertas de hardware y software a bajo precio, como también servicios para los usuarios de sitios web: hospedaje (hosting), registro de dominios, optimización de sitios web y así por el estilo.

Ejemplos:

Tema: Grandes ahorros en software OEM. Todas las mejores marcas a tu disposición.

¿Buscas software de alta calidad a bajo precio?
Nosotros tenemos lo que necesitas

Windows XP Professional 2002..... \$50
Adobe Photoshop 7.0 \$60
Microsoft Office XP Professional 2002.... \$60
Corel Draw Graphics Suite 11 \$60

y mucho más...

Finanzas personales

El spam de esta categoría ofrece seguros, servicios de reducción de deudas, préstamos con bajos intereses, etc.

Ejemplos:

Tema: Los prestamistas compiten entre sí...tú ganas.

Reduce tus pagos de hipoteca.

¡Los intereses están creciendo!
Dale a tu familia la libertad financiera que se merece.

Refinancia hoy y ahorra.

- *Rápido y fácil
- *CONFIDENCIAL
- *Cientos de prestamistas
- *100% gratis
- *Obtén las mejores tasas

¡Solicítalo hoy! {ENLACE}

Cualquier crédito será aceptado.

Para borrar tu nombre de nuestra base de datos pulsa aquí Gracias.
Gracias.

Llama 1-800-279-7310
o escríbenos a:
1700 E. Elliot Rd. STE3-C4
Tempe, AZ. 85283

Educación

Esta categoría incluye ofertas de seminarios, entrenamientos y diplomaturas en línea.

Ejemplos:

Tema: Obtén un diploma de licenciatura o doctorado desde tu casa.
Llama a {número de teléfono} para averiguar sobre nuestros programas de graduación.
Si estás buscando un grado de licenciatura, doctorado o MBA
Podemos darte credenciales completamente verificables para que hagas carrera. BACK ON TRACK!
Sin exámenes ni tesis. Llama: {Teléfono} Call: {Phone Num.}
nos disculpamos si no querías recibir este mensaje.
Para darte de baja de nuestra lista, por favor llama {Teléfono}

¿Quién lo utiliza?

El cartero comercial se cuela en los portales para atiborrar los buzones de publicidad. Pero, además de costar dinero, su radio de acción es muy limitado. ¿Por qué no utilizar el correo electrónico? Las empresas se dieron cuenta que a través del e-mail se pueden enviar más mensajes, a mucha más gente, mucho más lejos y por muy poco dinero.

Basta con hacerse con un listado de direcciones, escribir un mensaje genérico y disponer de un módem a 28.8 Kbps para mandar cientos de miles de mensajes por hora. Lo que no consideró el spammer es que ese sistema se acabaría convirtiendo en una auténtica plaga de la red, que inunda servidores, congestiona la red y desespera a los usuarios.

¿Cómo consigue las direcciones?

Hay muchos métodos bastante sencillos de confeccionar una nutrida base de datos con direcciones de correo. Un e-mail lleva, como mínimo, las direcciones del emisor y receptor. Cualquiera que monte un servidor de correo podrá acumular las direcciones de todos los correos que pasen por él. USENET es una fuente inagotable de direcciones de correo, y no sólo para el que tenga acceso al servidor, basta con bucear entre los grupos de noticias para coleccionar direcciones.

Las arañas que rastrean Internet, igual que buscan URLs, también pueden localizar direcciones de correo electrónico. Así que si ha participado en un foro de discusión o tiene la dirección en alguna página de la WWW, es bastante probable que caiga en manos de un spammer.

Con todas esas facilidades ya sólo queda montar una empresa con la malsana intención de acumular direcciones de correo electrónico para vendérselas al mejor postor.

¿Por qué es un problema?

El spammer dice: 'pero si basta con borrar el mensaje'. A lo que bastaría con contestar: 'es que no tengo por qué recibir ese mensaje'. Pero el problema es bastante más grande que el tiempo que lleva apretar la tecla 'delete'. El anunciante-spammer ahorra mucho dinero utilizando este método, pero el precio de su publicidad lo acaba pagando con creces la comunidad de Internet.

Un ISP tiene que gastar mucho tiempo procesando el spam, lo que afecta directamente al tiempo para procesar el correo 'normal'. Si se quiere defender utilizando un filtro, el tiempo que tardará en filtrar la basura, será todavía mayor. Por eso, la mayoría de ISPs descartan los filtros como método efectivo de lucha contra el spam.

Además, un ISP compra ancho de banda dependiendo del número de usuarios que se conectan a través de él. Para los proveedores pequeños, la inversión en ancho de banda se lleva el mayor pellizco de su presupuesto. Un uso razonable de esa conexión conlleva normalmente el incremento de la calidad del servicio y del número de usuarios. Pero cuando las líneas las empiezan a ocupar extraños (spammers), el ISP debe elegir entre que sus verdaderos usuarios tengan una conexión más lenta, pagar por más ancho de banda o subir las tarifas. Al final el receptor paga por el spam lo que el emisor se ha ahorrado.

AOL, por ejemplo, recibía 1,8 millones de mensajes al día de Ciber-promociones hasta que consiguió una orden judicial para prohibirlos. Si a un usuario le lleva unos 10 segundos identificar el correo basura y tirarlo, sólo en AOL se gastaban más de 5.000 horas de conexión al día por culpa del spam.

El spam, en resumen, utiliza un montón de recursos ajenos que otros acaban pagando. Además oculta al e-mail

con verdadero valor, al que le cuesta más sacar la cabeza en el cenagal del correo basura.

Spammer y mentiroso

Como 95% de los usuarios rechazan de plano recibir mensajes no solicitados, el spammer debe ingeniárselas para que su mensaje no sea descartado a la primera de cambio. La práctica más primitiva consiste en que el 'Asunto' parezca cualquier cosa menos un anuncio.

Para evitar los filtros que colocan los usuarios en sus buzones, los spammers utilizan trucos para disfrazar el origen del mensaje. Una estrategia habitual consiste enviar los e-mails a través del servidor de un tercero que, para colmo, es el que sufrirá las iras de los usuarios-víctimas.

¿Qué hay dentro del spam?

Hay lugares de la red donde usuarios y administradores de sistema pueden reenviar el spam para acumular datos sobre de donde proviene. Listas de correo como SMAP-L@EVA.DC.LSOFT.COM o en USENET dentro de news.admin.net-abuse.* estudian el spam para fichar a las empresas que hacen publicidad vía UCE (Unsolicited Commercial Email; correo electrónico comercial no solicitado) y analizar el contenido de los mensajes. El spam mas corriente incluye:

- Cadenas de cartas. Esas de 'reenvíelo a 10 personas y sobrevivirá'.
- Negocios piramidales, incluido el Multilevel Marketing (MLM).
- Otros mensajes tipo 'Hágase rico rápidamente'.

- Anuncios de webs pornográficas o líneas eróticas.
- Programas para acumular direcciones y hacer spamming.
- Oferta de acciones de empresas desconocidas.
- Remedios milagrosos.
- Niños/Ancianos muy enfermos. Penurias y tragedias varias.
- Falsas amenazas de virus.
- Programas piratas (warez).

Armas contra el spam

Ante el spam el usuario puede resignarse (o mentar a la madre del remitente) y borrar el mensaje o combatirlo. Lo fundamental, es, por lo menos, no contribuir a su difusión. Así, por ejemplo, no reenviar a x personas mensajes del tipo Pirámide-Virus-Niño Enfermo, ni contestar para darse de baja de alguna supuesta lista de distribución (lo que sólo servirá para que el spammer confirme que la dirección está activa).

Para tratar en lo posible que no inunde nuestro correo, en la red se pueden encontrar muchos programas anti-spam que utilizan diversas técnicas de filtrado.

Combatir el spam con mail-bombing o armas similares sólo contribuye a engordar el problema. Sin embargo, rechazar el spam de plano, quejarse a listas y webs *ad hoc* o al los responsables del servidor (se puede probar con `postmaster@dominio`, `root@dominio` `admin@dominio`) a veces resulta útil.

En USENET se ha tratado hasta de aplicar la pena de muerte (Usenet Death Penalty) contra proveedores como Netcom o UUNet, usuales emisores de spam, que consiste en ponerse de acuerdo para no aceptar mensajes de estas máquinas. Pero no funciona, porque los spammers cambian rápidamente de proveedor.

La USENET española, por ejemplo, está controlada por filtros, a través de los dos principales servidores de grupos de noticias: RedIris (para las universidades) e Ibernet (para los proveedores). RedIris filtra los correos mayores de 300 Kbytes e impide enviar un mismo mensaje a más de 10 grupos (*crossposting*). En Ibernet no se aceptan archivos binarios (fotos, programas) que no sean para grupos específicos, no se puede hacer *crossposting* a más de 14 grupos ni enviar mensajes de más de 1Mb.

El popular correo electrónico de Microsoft, Hotmail, acaba de anunciar que filtrará todos los mensajes que procedan de servidores que estén en lista negra del Mail Abuse Prevention System's (MAPS). El Congreso Estados Unidos también anda a vueltas con aprobar una ley anti-spam, pero no da con una fórmula que satisfaga a todas las partes. En California se ha aprobado una ley que obliga a los spammers a borrar de sus listas a quien lo solicite y otra que faculta a los ISP a cobrar multas de 50 dólares por cada correo basura mandado desde sus máquinas.

Qué hacer con el Spam?

Situación

Con la probabilidad de que casi el 12% del correo no solicitado sea respondido, es factible que aumente el recibo de información no solicitada a su buzón electrónico.

Medidas preventivas básicas

Aunque las acciones a tomar realmente tienen que ver más con la personalidad de quien recibe el mensaje, considero que el tiempo invertido en combatirlo es completamente perdido, por lo tanto sugiero que simplemente borre el mensaje de su buzón y suponga que no lo recibió. Muchos de estos son distinguibles a

simple vista porque incluyen o el signo de pesos, o valores en el encabezado. Otros incluyen las palabras GRATIS o FREE igualmente.

Recomiendo entonces, no tener en cuenta estos mensajes y hacer lo que hacen el 55% de los usuarios de la red: los borran. En caso de que el volumen de mensajes sea muy alto (10 o más al día) sugiero tomar otro tipo de medidas que pueden ir desde la solicitud de ser removido de las listas hasta la difusión de la información del infractor.

Hay que tener presente que los autores del spam cuentan con herramientas muy sofisticadas para recolectar direcciones E-mail válidas, entre ellas podemos citar los programas *webspiders* que permiten rastrear páginas web, news y otros recursos de Internet. Por lo tanto:

Sólo hay que dar nuestra dirección E-mail a nuestros amigos y conocidos.

No publicar nuestra dirección E-mail en las News o en páginas web.

No rellenar formularios en los que se soliciten nuestros datos personales.

Nunca hay que contestar a un mensaje de spam ya que en muchos casos la dirección del remitente será falsa y nos devolverán el mensaje y si no es falsa servirá a la empresa de publicidad para saber que nuestra dirección E-mail es correcta.

Los programas de correo suelen incluir sistemas de filtrado de mensajes que pueden ser útiles para evitar el spam. Es la solución de andar por casa para tener un programa anti-spam sin gastar dinero.

Aparte de estas recetas caseras, nunca está de más disponer de herramientas más sofisticadas que nos ayuden a evitar este tipo de correo masivo en nuestro buzón.

Programas Anti-Spam

Los programas que vamos a comentar son *shareware* o *freeware*. Aunque no están todos los que existen, éstos son los más conocidos y pueden encontrarse en cualquier web especializado en *shareware*.

La mayoría sirven tanto para evitar el *spam* como el *mail-bombing*. Este tipo de programas utilizan en general diversas técnicas, tales como enviar mensajes al postmaster del dominio del que procede el spam o borrar directamente los mensajes sospechosos de nuestro servidor de correo para evitar descargarlos. Son por lo tanto herramientas que hay que utilizar con precaución y mucho cuidado.

***AntiSpam 1.0* <http://www.xde.net/antispam>**

Programa anti-spam que cuenta con el aliciente de que su base de datos sobre spammers se va actualizando periódicamente a través de Internet.

***Bounce Spam Mail 1.8* <http://ay.home.ml.org/bsm>**

Envía mensajes falsos a los spammers indicando que nuestra dirección de correo no existe. El objetivo es que nos den de baja en su lista de correo. Un buen sistema para evitar los mensajes de nuestro peor enemigo. Dudo mucho de la utilidad de este sistema.

***CYBERSitter Anti-Spam 1.0* <http://www.solidoak.com/antispampg.htm>**

Permite seleccionar el E-mail que queremos recibir por palabras clave, dominio, dominios inexistentes y otros filtros.

***Deadletter 1.12* <http://www.deadletter.com>**

Se trata de un módulo anti-spammer específico para Eudora Pro y Light 3.05 o superior. Lleva la consabida lista de spammers y otras opciones de filtrado.

E-Mail Remover 2.4 <http://home.pacific.net.sg/~thantom/eremove.htm>

Permite ver las cabeceras de los mensajes en el servidor antes de descargarlos, permitiendo su eliminación. Puede que no sea el mejor, pero tiene el aliciente de que es Freeware (gratuito).

MailShield 1.0 <http://www.mailshield.com>

Una auténtica barrera que filtra el spam y el mail-bombing en el servidor antes de que lo recibamos.

MailTalkX 2.3 <http://www.softbytelabs.com/MailTalkX>

Además de ser una herramienta anti-spam efectiva permite monitorizar nuestro E-mail con todo tipo de filtros y avisos. Permite el control total sobre todas las cuentas de correo que queramos. Está considerado como uno de los mejores programas anti-spam.

Spam Bait Creator 1.0 <http://pw2.netcom.com/~p.sheedy/spambaitcreator.html>

Crea páginas web con direcciones E-mail falsas, de forma que al ser rastreadas por los webspiders de los spammers sean registradas en su base de datos. Nosotros no lo veremos pero nos divertiremos al menos al pensar en la cara del spammer. Programa Freeware.

Spam Exterminator 3.2f <http://www.unisyn.com/spamex/SpamEx.htm>

Permite ver las cabeceras de los mensajes en el servidor y eliminar el spam. Incluye una lista de spammers, filtros diversos. Incluso permite responder de forma automática a los spammers diciendo que no nos gusta su conducta (una mala idea, como ya sabemos).

Spam Hater 2.08 http://www.cix.co.uk/~net-services/spam/spam_hater.htm

Programa Freeware que se integra en nuestro cliente de correo o lector de news para responder al spam. Responde a postmasters de los dominios con spammers que no nos gustan sus mensajes. La idea es que algunos dominios no permiten la realización de spam y los darán de baja. Sinceramente no creo que esto sirva de mucho, pero es una forma de ejercer nuestro derecho al pataleo de forma automática.

SpamBuster 1.61 <http://www.contactplus.com>

Se trata de una de los programas más conocidos de este género. Funciona con el tradicional sistema de filtros, bajando únicamente las cabeceras de los mensajes para evitar perder tiempo.

Nuevas formas de spam

En los últimos días hemos recibido algunos mensajes no solicitados con características nuevas y muy molestas.

La imaginación de los spammers nunca descansa.

A lo molesto que resulta recibir sus mensajes no solicitados sobre cosas que no nos interesan, ahora han agregado algunas características bastante insufribles.

La primera es que cuando recibimos el mensaje (en formato HTML) y lo seleccionamos para leerlo el navegador se abre solo y conecta con la página del spammer.

Esto es absolutamente detestable. Además de soportar mensajes indeseados hay que aguantar que los spammers decidan qué programas se abren en nuestra computadora.

La segunda consiste en enviar un mail engañoso como el que sigue:

[Asunto: lo que me preguntaste

Me lo pasaron en la oficina en
www.nombredelaempresa.com
podes registrar gratis tu dominio y te dan hosting y mails con dominio
propio.
Fíjate que puedes tener 2 meses gratis de hosting y te dan \$100 en servicios
yo puse la pagina ahí!!!!!!

Míralo y cuéntame!!!!!!

Besos

Ah me olvidaba cunado hables con Juan dile que me llame!!!! (Vos
entended!!)]

Este mensaje pretende engañarnos, como si el remitente hubiera querido enviárselo a un conocido y se hubiera equivocado y nos lo hubiera enviado a nosotros.

Con el tono personal que se le da al mail pretenden hacernos creer que el remitente realmente hubiera querido enviarlo a otra persona.

Aclaro que yo no conozco a ninguna de las personas que aparecen en el mensaje ni en el remitente, ni hablé con nadie sobre el tema al que hace referencia el mail por lo que es obvio que no estaba dirigido a mí.

Si alguien protestara seguramente le dirían que fue solamente una equivocación, pero esto no es verdad porque he recibido varios de estos mensajes provenientes de distintas empresas y conozco a varias personas que también han recibido mensajes de esta clase



Además, tenga en cuenta las siguientes directrices para protegerse del *spam* y minimizar sus efectos:

No publique sus direcciones de correo electrónico personales en ningún sitio público, como por ejemplo páginas web.

Nunca pulse sobre el enlace unsubscribe de un mensaje de *spam*. Lo único que conseguirá es que el *spammer* verifique que su dirección de correo está activa.

No responda nunca a un mensaje de *spam*.

No reenvíe cartas encadenadas, peticiones o alertas de virus dudosas.

No abra el mensaje de *spam*.

Deshabilite la *Vista Previa* de su cliente de correo electrónico.

No realice compras de productos que le hayan llegado a través de mensajes de correo no solicitados.

Disponga de varias cuentas de correo electrónico, y déles usos separados: personal, trabajo, etc.

Utilice un filtro anti-*spam* o una solución anti-*spam*.

Instale una solución antivirus.

Instale un *software* de filtrado de contenidos.

Desde Panda Software ponemos a su disposición varias soluciones que le mantendrán a salvo del *spyware*, además de otras amenazas como virus, *hackers* y *phishing*.

Visite nuestra tienda para adquirir la solución Panda más adaptada a sus necesidades.

Descargue una versión de evaluación de nuestros productos para poder probarlos antes de comprarlos.

Utilice Panda ActiveScan, la solución gratuita online de Panda Software, que detectará las amenazas presentes en su ordenador.

Conclusión

Si el spam continúa creciendo a la velocidad que lo está haciendo, Internet pronto transportará mucho más Spam que verdadero correo. La circulación del Spam la paga el receptor. Se necesita mayor ancho de banda y a menudo los sistemas de correo deben ser actualizados para poder manejar el Spam.

En muchos países las leyes no ayudan mucho a la gente para protegerla contra los delincuentes spammers. De hecho algunos países cuentan con leyes que restringen únicamente a la gente honesta (administración de derechos digitales, etc....) y ayudan a los delincuentes (por ejemplo, a conseguir lindas estadísticas acerca del correo spam).