El SPAM no sólo es un problema para los usuarios de Internet que reciben diariamente en sus buzones docenas de e-mails no deseados en los que se les oferta variados artículos para aumentar su potencia sexual o conseguir una tupida melena. También es un problema muy serio para las empresas que ven cómo sus correos publicitarios o comerciales por algún misterioso motivo son catalogados como SPAM y no llegan a sus clientes.

Recuerdo el caso de una empresa que tras varios años realizando inadecuadas campañas de e-mailings para captar y fidelizar clientes, acabó consiguiendo que el 75% de sus correos fueran catalogados como SPAM y nunca llegaran a su destino. Los responsables de marketing se reunieron y tomaron una decisión: había que comprar un ordenador con una capacidad 100 veces mayor de envío de correos. Por supuesto aquello no funcionó.

Lo primero que debe conocer son los **dos motivos** principales por los que sus correos pueden ser catalogados como SPAM:

1. Los destinatarios de sus correos no **deseaban recibirlos** o **no son capaces de visualizarlos** correctamente y realizan una denuncia de SPAM en las listas **RBL** (listas negras publicas internacionales).
2. Sus correos son detectados automáticamente como SPAM por un **filtro Bayesiano**.

Si quiere saber cómo evitar que sus e-mails sean catalogados como SPAM le recomiendo que lea el siguiente artículo de HelloGoogle.com donde detallo consejos muy concretos y prácticos, que le ayudaran a optimizar el ratio de recepción de sus campañas de Marketing:

1. Filtre su base de datos de e-mails para evitar envíos innecesarios.

- **Elimine e-mails incorrectos** de su base de datos. Los correos del tipo aa@aa.es son fácilmente descartables.
- Ofrezca un servicio para que sus clientes puedan **actualizar sus correos**: Más del 30% de sus clientes podrán cambiar de correo a lo largo de un año.
- Utilice **servicios de *list hygiene***: Más del uno por ciento de sus correos serán direcciones mal formadas del tipo johngmail.com que claramente deberían ser john@gmail.com. Las aplicaciones de list hygiene son capaces de corregir este tipo de errores de sus bases de datos.
- **Elimine de su base de datos direcciones de correo "*Spam flag*"**: Se trata de direcciones de correo que se han añadido de manera malintencionada y que pueden hacer que su empresa se autodenuncie en listas negras. Por ejemplo: abuse@somedomain.

2. Tenga presente la siguiente guía de Buenas prácticas para obtener el permiso de las personas que recibirán sus e-mails.

- Realice el **sistema de suscripciones más conservador** que pueda permitirse: Antes de incluir una dirección de correo en su base de datos, la mayoría de las empresas envían a sus suscriptores un correo de confirmación en el que se solicita que confirmen su interés en recibir información comercial por correo.

- Conserve **la dirección IP de sus suscriptores**: Le permitirá cubrirse las espaldas en el caso de que se vea en la necesidad de conversar con ISPs y Listas negras.
- Evite comprar listas de e-mails, y si lo hace, investigue la fuente de estas listas. Puede recurrir a un *trustworthy list broker* para que le asesore en la adquisición de una lista de calidad.
- Permita que sus clientes puedan **desuscribirse de manera clara, sencilla y rápida**.

3. Elija el ISP de su servidor de correo cuidadosamente.

Si su ISP ha sido denunciado a una blacklist, los correos que envía a través de sus servidores serán catalogados como SPAM. Puede apuntarse a la siguiente lista de discusión sobre SPAM http://peach.ease.lsoft.com/archives/spam-l.html donde podrá buscar ISP de confianza.

4. Cuide minuciosamente el contenido del Subject y cuerpo de sus correos para evitar los filtros anti-spam por contenido o filtros Bayesianos.

Los filtros Bayesianos aunque representan la última técnica en la lucha contra el SPAM se basan en un método estadístico descubierto en el siglo XVIII, por el clérigo y matemático Thomas Bayes, (1701-1761). La estadística bayesiana es una herramienta muy eficaz para poder calcular la probabilidad de que ocurra un suceso determinado, en nuestro caso que un e-mail sea SPAM. Para realizar este cáculo estadístico nos basamos en la experiencia de lo ocurrido anteriormente en casos semejantes.

Para evitar que nuestros e-mails sean catalogados como SPAM por un filtro Bayesiano es importante que conozcamos cómo funcionan: Cuando un ISP recibe un email y una persona determina **manualmente** que se trata de un caso de spam, se observa la **frecuencia** relativa de cada una de las palabras del mensaje, se calcula su **probabilidad** de ocurrencia y se actualiza el filtro Bayesiano con esta información. También se hace exactamente lo mismo con los mensajes que se reciben y son considerados como no spam.

Cuando ya hemos entrenado a nuestro filtro Bayesiano con muchas palabras asociadas a la práctica de spam y no-spam, podemos pedirle que calcule de manera automática la probabilidad de que cada e-mail que se reciba sea o no sea spam en función de las palabras que contiene, por ejemplo *"viagra" ó "gratis", "enlarge"*. Así se calcula la probabilidad de que el mensaje sea spam. A esta cifra se le llama *"spamicidad" y* cuando supera un umbral (por ejemplo el 90%), se puede clasificar de manera segura como spam.

Una vez entrenado, un filtro Bayesiano ofrece muy pocos *falsos positivos,* ya que a diferencia de otros filtros, ataca la esencia del problema del spam: el contenido del mensaje. Recuerde que el método bayesiano es multilingüe e internacional, un filtro anti-spam bayesiano, al ser adaptable, puede utilizarse con cualquier idioma.

Por tanto, para evitar los filtros Bayesianos debe prestar especial atención al contenido y redacción de sus e-mails:

- Evite utilizar un estilo demasiado **comercial** en la redacción de sus contenidos.
- Evita las expresiones y palabras demasiado **agresivas** como “FREE”, “*GRATIS*“, “*COMPRE AHORA*” o “*DESCUENTOS*“.
- No escriba **nunca en mayúsculas** en el Subject.
- Evite el **uso excesivo de signos de admiración o símbolos** como $$.
- Evite la utilización de la frase **“haga click aquí ”.**
- Evite las **frases redundantes** y las instrucciones **poco concisas**.

Además, las más avanzadas soluciones en materia anti-spam incluyen un motor de filtro bayesiano de segunda generación, lo que supone no sólo un simple análisis de texto, sino también un amplio exámen de la forma y los atributos de los archivos adjuntos.

Si tiene curiosidad por ver cómo funcionan los filtros bayesianos, puede descargarse el programa gratuito anti SPAM K9 desde esta dirección.

5. Cuide el código HTML de sus e-mails:

- Evite las imágenes de fondo, en muchos webmails no se visualizarán.
- No ponga texto editable sobre las imágenes de fondo, pues al desaparecer la imagen perderán su contexto.
- Todas las imágenes deben tener la etiqueta “ALT” y “TITLE” con su correspondiente texto descriptivo.
- No utilice hojas de estilo CSS externas, ni declare los estilos en la cabecera pues algunos webmails los eliminan.
- Aplique los estilos CSS directamente sobre los tags (style=”…”).
- Utilice tablas para la maquetación de sus contenidos.
- Evite los layouts líquidos .
- Evite siempre incluir controles ActiveX
- No utilice imágenes animadas ni flash.
- Incluya siempre el charset para la definición de los caracteres en el idioma correspondiente.

6. Configure correctamente su infraestructura de envío de e-mails:

- Mantenga Activado la **resolución inversa de DNS**: Muchos filtros de correo utilizan la resolución inversa para asegurarse que la compañía que se supone está enviando los e-mails es realmente el emisor. En el caso de que no esté activa, sus correos no se enviarán.
- Compruebe si mantiene **Relays abiertos** en su servidor de correo y **ciérrelos**: Los Spammers a menudo buscan relays abiertos para enviar sus correos a través de los servidores de correo de otras compañías.
- No haga **relay entre servidores** antes de enviar los correos: Los correos de algunas empresas suelen viajar entre varios servidores internos antes de entregarlos al destinatario final; ésto podría ser irrelevante si no fuera porque el relay entre servidores es una práctica habitual entre los Spammers para intentar ocultar la procedencia de sus correos. Tenga en cuenta que cuanto menos relay haga, menos dudas habrá sobre la procedencia de sus correos.
- Utilice un **formMail seguro** en su página web: Un agujero de seguridad en su formulario de envio de correos puede ser una puerta abierta para que los Spammers envíen información desde su servidor de correo.

7. Monitorice constantemente su sistema para saber si está ocurriendo un problema. Hay varias formas de saber cuándo hay un problema en la entrega de los correos:

- Monitorice los **ratios de entrega** por dominio: De esta manera puede comprobar por ejemplo si hay una caida en los ratios de entrega de correos de GMail.
- Monitorice sus campañas de e-mails **antes de comenzarlas**: Antes de lanzar una campaña es importante asegurarse que nuestros correos serán aceptados por los principales ISP (en la práctica los 15 ISPs principales representan el 60% del mercado). Existen empresas de seguridad que ofrecen servicios de chequeo automático de e-mails para saber si sus campañas pasarán los filtros antispam de los principales ISPs.
- Monitorice las **blacklists**: Compruebe si su servidor de correo está dentro de alguna lista negra. Algunos sistemas de seguridad ofrecen un servicio de Blacklist Alert que le alerta si su servidor de correo se encuentra en más de 300 blacklists.

8. Mantenga buenas relaciones con los ISPs.

Siempre es de ayuda saber a quién dirigirse cuando hay un problema, pero recuerde que para mantener una buena relación es importante dedicarle mucho tiempo y recursos.

9. Y por supuesto, no haga SPAM.

El envío masivo e indiscriminado de e-mailings a personas que no los han solicitado, no le harán incrementar sus ventas. Por el contrario dañara la imagen de su empresa y tarde o temprano acabará originándole serios problemas.

Espero que con la ayuda de estos consejos sus campañas de e-marketing acaben llegando siempre a buen puerto.

 IGNACIO GOROSTIZA

http://www.hellogoogle.com/como_evitar_filtros_anti_spam/