Consejos para evitar que tus emails lleguen como SPAM

Todo el mundo habrá pasado por la situación de haber enviado un correo electrónico a alguno de sus contactos y al tiempo enterarse de que dicho correo no ha llegado, o directamente ha sido archivado por el gestor de correo del destinatario en la carpeta de spam. En ese momento te preguntas qué puede haber pasado para que ese correo haya sido marcado como spam.

Los factores que pueden influir son muchos. A lo largo de este White Paper veremos qué medidas podemos tomar para evitar esta situación, sobre todo cuando queremos hacer un envío de Email Marketing.

¿Qué es el correo Spam o no deseado?

Todo el mundo que está familiarizado con Internet tiene muy presente el concepto de correo SPAM o correo no deseado, pero nunca está de más recordar en qué consiste este tipo de emails que recibimos en nuestro buzón a diario, y en muchas ocasiones, en número muy superior al que nos gustaría recibir.

Podemos decir, que el correo basura es una forma de inundar la red con miles de copias del mismo mensaje que son enviados a gran cantidad de direcciones, con la intención de que el usuario pueda ver la información que contiene el mensaje. El problema radica en que en muchas de las ocasiones estos mensajes son recibidos sin nuestro consentimiento. Se suele utilizar mucho para hacer un tipo de publicidad no deseada como anuncios comerciales, anuncios de pornografía o servicios que rozan la legalidad, por citar algunos casos.

Pero no todos los mensajes son con fines comerciales, sino que también nos podemos encontrar el caso de aquellos mensajes que son enviados para incordiar. En este grupo podemos incluir las cadenas de mensajes, información de falsos virus o falsos premios por reenviar el correo a tus contactos.

Por suerte, los filtros de antispam utilizados por los proveedores de correo electrónico, cada vez son más sofisticados, siendo capaces de filtrar de forma más fiable este tipo de envío, aunque los spammers también evolucionan buscando nuevos métodos para saltarse los filtros.

Motivos por los que el correo puede ser marcado como spam

Para determinar el motivo por el que nuestros correos pueden ser considerados como correo basura, es importante conocer cómo piensan los filtros que los analizan y que son los encargados de determinar si un correo es spam o no. En este aspecto influye tanto el asunto que pongamos como a quien va dirigido o el cuerpo del mismo. Hagamos un repaso por cada uno de los puntos que puede hacer que nuestro correo no llegue como deseemos.

a) Línea del asunto

El asunto de un correo puede ser el medio más rápido para determinar si se trata de un correo bueno o no, incluso si ha superado los filtros, dependiendo de la información que aquí venga, el destinatario lo abrirá o directamente lo enviará a la basura. Asuntos en mayúsculas, con signos raros, o que contengan palabras catalogadas como potencialmente peligrosas tipo “Gratis”, “Cupones” o “Hipoteca”, pueden hacer que nuestro email se marque como spam.

b) Campo “Para”

Los filtros tienen más consideración a la hora de analizar un mensaje si en este campo aparece el nombre y apellido del destinatario junto a su email. Es lo mismo que ocurre cuando en tu correo convencional recibes cartas publicitarias dirigidas al “cabeza de familia”. Para ello, a la hora de guardar las direcciones de email hazlo con el nombre y apellido del destinatario (por ejemplo, “Juan López”), mejor que algo genérico como “Departamento de Comunicación”.

c) Contenido del mensaje

El contenido es otro de los primeros campos que son analizados por cualquier sistema antispam. Si detectan que el contenido incluye palabras o frases que son comunes en los correos basura, será más fácil que se marque como correo no deseado.

d) Direcciones IP

Esto es un aspecto que está lejos de poder ser controlado por el usuario, ya que hay algunos filtros que se sincronizan con las denominadas listas negras, donde se registran esas direcciones IP desde las que se hacen envíos fraudulentos. Si la dirección IP de tu servidor de correo electrónico está en una lista negra, los filtros spam no dejarán pasar tu correo.

e) Dirección del correo del remitente

Hay otros casos en los que es necesario haber establecido un vínculo previo entre el que envía y el que recibe el correo, para que este no sea marcado como spam. Hay servidores que sí detectan que el correo desde el que se envía el email no ha sido añadido en una lista blanca como amigo, o si el

correo no aparece en su lista de contactos, será catalogado como extraño, por lo que lo más fácil es que sea marcado como spam.

f) Nombre del dominio

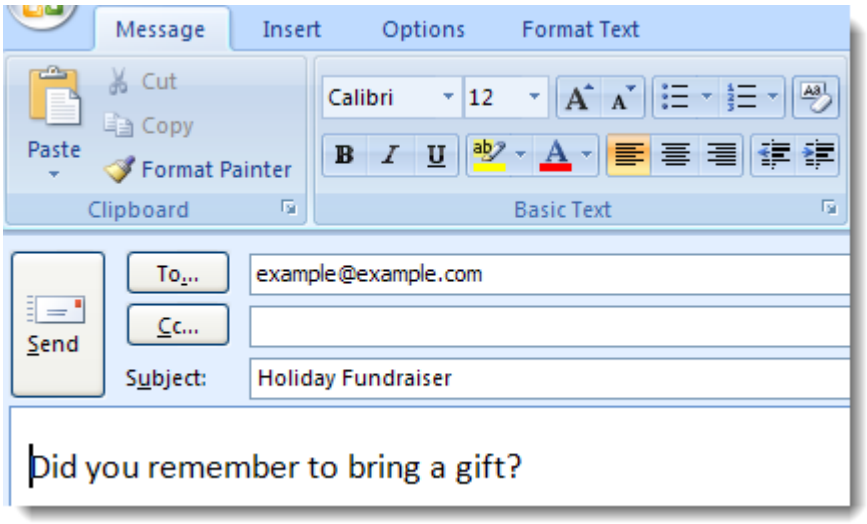
Cada vez es más habitual, que los servidores de correo verifiquen si realmente el email del que proviene el correo pertenece realmente al dominio indicado, y no se trata de una suplantación de identidad. Esto lo hacen con sistemas de verificación como DomainKesy o los registros SPF.

Consejos que debemos seguir para que nuestros emails no sean catalogados como spam

Teniendo en cuenta todo lo comentado, vamos a ver algunas recomendaciones a tener en cuenta a la hora de redactar nuestros correos para evitar lo máximo posible que nunca lleguen como spam.

1.- Cuidado al escribir el asunto y el contenido de los correos

Muchos servidores de correo utilizan los filtros Bayesianos para determinar si un correo es spam o no. Se trata de unos filtros que hacen uso de métodos estadísticos para clasificar el correo, y se basan en la experiencia de lo ocurrido anteriormente en casos semejantes.



Es muy importante conocer cómo funciona este tipo de filtros para evitar que marquen como spam nuestros emails. Cuando una persona marca de forma manual un correo como correo basura, se observa la frecuencia relativa de cada una de las palabras que forman parte del mensaje y del asunto. Se calcula su probabilidad de ocurrencia y se actualiza el filtro Bayesiano con esta información. Una vez que el filtro tiene esta información, le podemos pedir que calcule de forma automática la probabilidad de que un correo sea catalogado como spam o no. Cuando un mensaje supera un umbral determinado, por ejemplo el 90%, entonces podemos asegurar que se trata de un correo basura.

Si queremos evitar este tipo de filtros, es muy importante que pongamos gran atención a la información que acompaña al correo. Para ello podemos evitar:

- Utilizar un estilo muy comercial a la hora de redactarlo
- Utilizar palabras comunes que forman parte de los correos basura como “Free”, “Gratis”, “Viagra”…
- Escribir el asunto todo en mayúsculas

- Utilizar frases como “Pulse aquí”, “Haga clic aquí” o similares

2.- Cuida el código HTML del cuerpo del mensaje
Es muy habitual querer enviar emails con formato HTML, ya que estos resultan más vistosos, pero enviar la información de esta forma puede suponer un arma de doble filo si no lo hacemos bien.

Lo primero que nos debemos asegurar es que el código está bien formado. Si lo hacemos de forma descuidada, se puede entender que ha sido enviado por un spammer. No dejemos etiquetas sin cerrar o imágenes mal enlazadas.

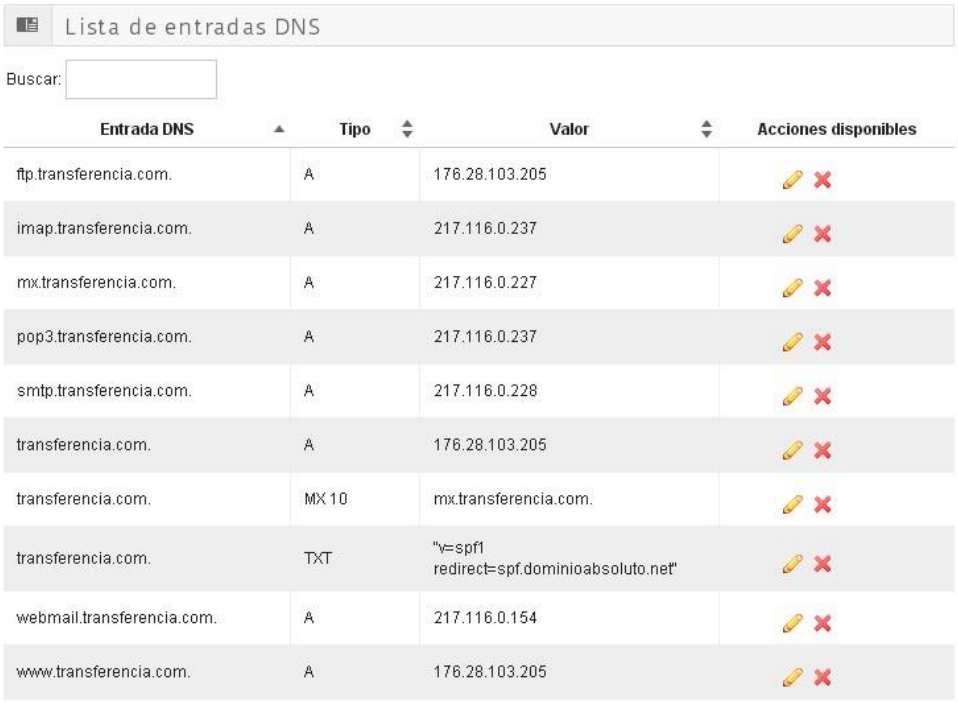
También es importante que añadamos un texto alternativo para aquellos casos en los que los destinatarios no pueden ver información en HTML. Si añades las dos opciones, puede ser un síntoma para los filtros de que no se trata de un spammer el que está haciendo el envío.

Tampoco nos decantemos por hacer uso de grandes imágenes que contienen toda la información, sin añadir ningún tipo de texto. Se trata de una técnica muy utilizada por los spammers, que añaden una imagen al cuerpo y se olvidan de meter texto. Añadir siempre algo de texto, aunque sea al final para dar las gracias.

3.- Dentro de lo posible, haz uso de una dirección IP dedicada
Internet se mueve por direcciones IP, de las que nos podemos encontrar dinámicas, que son las mayorías que ofrecen nuestros ISP o dedicadas, direcciones con un coste por su uso, pero con las que nos aseguramos que únicamente las estaremos utilizando nosotros.

La diferencia entre unas y otras a la hora de hacer el envío es que mientras las dinámicas pueden ser utilizadas por más de una persona (entre las que se puede encontrar alguien que haga envío de spam), las dedicadas sólo la estará usando una persona, por lo que es más difícil que sea metida en alguna lista negra.

4.- Revisa la buena configuración del servidor
Igual que es muy importante el contenido que acompañará a nuestros correos enviados, también lo es tener bien configurado el sistema de correo en nuestro servicio de alojamiento. Entre las cosas que podemos hacer es la de configurar la resolución inversa del DNS. Hay filtros que utilizan la resolución inversa para asegurarse de que la compañía que está realizando el envío es realmente quien lo hace, y no se trata de una suplantación de identidad.



Lista de entradas DNS

Buscar:

Entrada DNS	Tipo	Valor	Acciones disponibles
ftp.transferencia.com.	A	176.28.103.205	
imap.transferencia.com.	A	217.116.0.237	
mx.transferencia.com.	A	217.116.0.227	
pop3.transferencia.com.	A	217.116.0.237	
smtp.transferencia.com.	A	217.116.0.228	
transferencia.com.	A	176.28.103.205	
transferencia.com.	MX 10	mx.transferencia.com.	
transferencia.com.	TXT	"v=spf1 redirect=spf.dominioabsoluto.net"	
webmail.transferencia.com.	A	217.116.0.154	
www.transferencia.com.	A	176.28.103.205	

Un servicio similar al anterior es el registro SPF, que son las siglas de Sender Policy Framework, una protección contra las falsificaciones de correos electrónicos. Con el uso de este registro, estamos indicando desde qué servidores SMTP puede hacer envío nuestro dominio. Si lo hace desde alguno no especificado, el servidor de correo del destinatario lo podría rechazar.

5.- Nunca hagas spam

Esto que puede parecer una tontería, es uno de los principales fallos en los que cae la gente. Muchas empresas buscan sistemas para hacer llegar sus propuestas a los clientes, y para ello recurren al envío masivo a direcciones que no lo han solicitado. Esto a la larga puede traer muchos problemas, ya que puede hacer que la reputación de la compañía se vea dañada, además de conseguir meter su dominio en algún sistema de lista negra.