Consejos para evitar que tu correo llegue a spam

Hoy en día muchos proveedores de correo electrónico realizan un análisis adicional de los correos que provoca que puedan mandar ese correo a spam, en principio legítimo. Por ello el contenido en sí del correo electrónico que estás enviando también importa para que ese correo pueda ser considerado spam o no.

En este artículo vamos a tratar de recopilar los puntos más comunes por los que los usuarios ven que sus correos son clasificados como spam aunque esté todo correcto.

Las firmas en los correos electrónicos.

Las firmas de los usuarios se componen habitualmente de una dirección de correo, un nombre y a menudo se añaden enlaces o logos. Estos enlaces o logos pueden ser penalizados por muchos analizadores anti-spam. Especialmente si las imágenes se cargan desde recursos externos. Por ejemplo, muchos usuarios suben a dropbox una imagen y la insertan como firma. Este tipo de técnicas es fuertemente penalizado por muchos proveedores de correo electrónico.

Los enlaces en los correos

Los enlaces a menudo son fuente de este tipo de problemas. Especialmente si usas acortadores de direcciones. Frecuentemente se usan por los spammers para ocultar el destino real de un enlace malicioso

Correo electrónico escrito conforme a un estilo normal

No escribir asunto en el mensaje o escribirlo todo en mayúsculas puede llevar penalizaciones. Asimismo, hay combinaciones de palabras que pueden conllevar una detección en falso, especialmente en algunos sectores comerciales.

Enviar adjuntos sin texto también es algo a evitar. Si envías un archivo adjunto que se llame factura.pdf, añadir un asunto aclaratorio y un breve mensaje explicatorio en el mensaje evitará que 'parezca' spam.

Formato de los archivos adjuntos

Si quieres enviar archivos, es conveniente que los comprimas en un formato conocido. Por ejemplo, si quieres compartir una base de datos access o un documento de word, en lugar de adjuntarla directamente, es conveniente que la comprimas previamente. Hay proveedores que penalizan o incluso impiden entregar un documento .docx. Se deben evitar los formato en bruto de documentos de Microsoft Office como por ejemplo .xls, .doc, .xlsx, .docx, .ppt, etc.

Otros formatos comunmente penalizados:

- Los formatos de archivos ejecutables, como pueden ser los .exe.
- Los formatos de archivos de correo electrónico. Se debe evitar adjuntar correos en formato .eml, que es un tipo de formato común al reenviar

correo en algunos programas de correo electrónico

Verificar la configuración de la cuenta

A veces sucede que un usuario tiene la cuenta configurada contra varios proveedores. Esto puede suceder especialmente si has tenido un cambio de proveedores recientemente. Esta situación puede resultar en que envíes desde el proveedor anterior cuando deberías estarlo haciendo desde el proveedor nuevo. Puedes consultar la configuración de tu cuenta de correo siguiendo las instrucciones concretas de este enlace para tu programa de correo electrónico:

https://ayuda.guebs.com/category/correo-hosting/

Con algunos programas de correo como Apple Mail es sencillo confundirse y enviar con un servidor smtp inadecuado desde una de tus cuentas, resultando en correo marcado como spam o incluso correo rechazado.

Ocuparse adecuadamente del estado de tu correo

Es común que se dejen respondedores en marcha que responden a todo los correos que llegan. También responderían al spam que potencialmente podría llegar a la cuenta. Por ello es recomendable revisar las cuentas de correo que no se usen, los respondedores establecidos y las redirecciones creadas en los dominios.

En general hoy en día, es recomendable evitar redirecciones o autorespondedores. Ambos suelen generar problemas, en lugar de solucionarlos. Si estás redirigiendo tu correo a hotmail/outlook o gmail, estos proveedores permiten que configures tus cuentas para leer el correo desde sus interfaces. Puedes configurarlas para leer el correo en lugar de realizar redirecciones

Cómo leer tu correo de guebs desde Gmail

Como leer tu correo de guebs desde Outlook.com

Rebotes de correo

Cuando hacemos cualquier tipo de envío, es común que una dirección de una lista de las direcciones a la cual va dirigido ese correo falle. Entones, se genera un «NDR», Non Delivery Report. (https://en.wikipedia.org/wiki/Bounce_message En inglés) A menudo el asunto de estos correos es «Mail Delivery Report»

Este mensaje lo recibe el remitente y en el mensaje encontrará la razón por la cual el correo ha sido rechazado. Leer este tipo de correos ofrece mucha información por la cual el sistema de correo destino ha decidido que tu correo no sea aceptado. Normalmente el mensaje contendrá un código de error y un mensaje explicando la causa, además de una copia parcial o completa del correo que se ha enviado.Por ejemplo

```
  SMTP error from remote mail server after RCPT TO:unacuenta@decorreo.com:
    550-5.2.1 The email account that you tried to reach is disabled
```

Tal y como se ve el proveedor que ha creado este rebote está informando de que la cuenta está deshabilitada

El envío recurrente a cuentas no existentes o deshabilitadas puede conllevar que un proveedor de correo disminuya la reputación de tu correo electrónico en general. Es, por lo tanto, necesario, revisar este tipo de rebotes y no ignorarlos: dentro de ellos se encuentran los problemas que el dominio puede tener.

Notificaciones de lectura

Las notificaciones de lectura , cuando están activadas, sirven para informar al remitente de que un correo ha sido leído. Si un usuario recibe mucho spam y lo abre para examinarlo, entonces el usuario envía un «Leído» con un asunto

típicamente spámico a la dirección remitente, que puede haber sido hackeada o impersonada desde otro lugar.

– Podría informar a un potencial spammer sobre la presencia de un 'humano' detrás de la cuenta, es decir, es una cuenta activa.

– A menudo, además, tener activadas estas notificaciones supone que cuando se borra un correo se envía un mensaje de «No leído:» lo que agrava todavía más la situación. Si un usuario decide borrar 100 correos de spam, enviará 100 notificaciones de «No leído»

Por ello es recomendable desactivar la notificación de lectura automática. Y que sólo se envíe cuando el usuario lo decide manualmente

Añadir como contacto a direcciones recurrentes

A menudo los grandes proveedores de internet como hotmail, gmail, etc. priorizan el correo de aquellos remitentes que un usuario expresamente ha deseado conocer. Por ello, si añades como contacto en dichos proveedores a la dirección remitente, su entregabilidad general mejorará. Cuantos más usuarios añadan tu cuenta como contacto, mayores mejoras en entregabilidad se producirán en el correo que envíe tu dominio.

Boletines o correos masivos

En estos envíos hay que tomar en consideración muchos puntos:

La dirección desde la que se envía este correo tiene que existir y tiene que ser revisada. Es fundamental revisar los rebotes de cualquier envío de correo masivo. La causa consiste en que si no se revisa suceden dos cosas: que los usuarios que quieren ser delistados y que respondan al remitente solicitándolo seguirán recibiendo envíos y que las cuentas que hayan dejado de existir no serán eliminadas de la lista.

Además, si el remitente de la campaña no puede recibir correos, entonces el envío será todavía más 'spámico'. Ésta es una regla común para todo envío

Si no se eliminan las direcciones inactivas/erróneas/mal escritas de la lista,

entonces la lista acabará siendo un enviador de correos fallidos. Esto es muy fuertemente penalizado por muchos proveedores de correo electrónico. Si tu porcentaje de correo fallido es elevado, entonces probablemente tus correos verán como la entregabilidad disminuye rápidamente. Un porcentaje mayor de un 1%-4% en los fallos en un envío masivo puede provocar problemas dependiendo del proveedor.

Al usuario al que se le envía este boletín se le tiene que informar de que forma parte de una lista, de qué empresa/organización le está enviando la comunicación, de un proceso claro y sencillo de delistado y de si el correo es publicitario o de otro tipo.

Si un proveedor detecta que sus usuarios reciben correo que no quieren (porque tienen la opción de marcar como spam, porque lo incluyen en filtros de bloqueo, o porque el usuario se queja) tu correo se verá fuertemente perjudicado.

En este punto se han de tener en cuenta las diferentes jurisdicciones. Por ejemplo, es de especial relevancia la ley CAN-SPAM, que presente direcciones a seguir por cualquier dominio que quiera enviar correo comercial en jurisdicción estadounidense:

https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Reevaluar la membresía de los usuarios en tus listas de envío (OPT IN)

En los envíos masivos de correo, hay que revisar los rebotes para eliminar a los usuarios cuyas cuentas ya no existen, para delistar a quienes lo soliciten y para solucionar cualquier problema que pueda surgir. Los rebotes son información valiosa que debe ser revisada para corregir un problema latente.

Pero además, muchos usuarios no solicitarán el delistado y marcarán continuamente tus correos como spam especialmente si la lista lleva mucho tiempo enviando correo sin supervisar. Es recomendable en estos casos hacer una campaña de re-suscripción. Es decir, enviar un correo a todos tus miembros de la lista indicándoles que **confirmen** de nuevo la subscripción a tu lista. Si no lo hacen, se les elimina.

Este es un modo rápido y eficiente de limpiar una lista de correo que no ha sido correctamente atendida en el pasado.

Listas basadas en adherencia únicamente

Algunos usuarios recogen listas de correo de fuentes de terceros porque desconocen lo que esto significa. Usar una de estas listas acabará con tus envíos en spam al 100%. Es mucho más adecuado construir tus listas de envío en base a usuarios que **piden** figurar en ellas. Si tus usuarios piden figurar en las listas, el ratio de marcado como spam será extremadamente bajo, lo que ayudará a que tus usuarios reciben mejor los envíos, resultando en una efectividad mucho más elevada que enviar a una lista de correos arbitraria.

Aspectos relacionados con cómo se envían los boletines: recipientes y software de envío

Muchos usuarios hacen envíos de correos enviando un solo correo y poniendo en el «Para:» a todos los destinatarios. Esto supone un problema por las siguientes razones

– Todos los usuarios de tu envío ven las demás cuentas de correo electrónico a las que envías el correo electrónico. Esto es un problema de privacidad que se debe evitar. Que se envíe un correo publicitario no tiene que derivar en que otros usuarios vean a los miembros de la lista en cuestión.

– Muchos proveedores bloquean o penalizan a aquellos usuarios que les envían muchos recipientes en un solo correo. En general esta práctica debe ser evitada

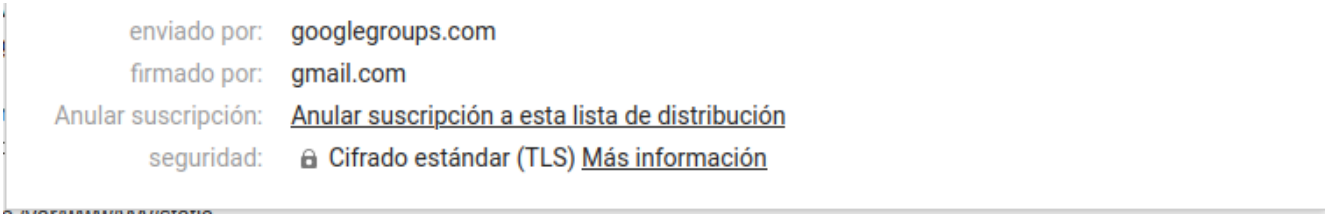
Para hacer un envío del modo correcto, se debe enviar 1 único correo a cada destinatario según las normas de los epígrafes anteriores de esta guía. Hay mucho software hoy en día que se ocupa de gestionar las listas automáticamente. Tanto en forma de plugins para wordpress, como en forma de software especializado para el envío de boletines informativos: mailman, phplist, etc.

Headers para listas de envío: List-Unsubscribe

En los últimos años ha ganado mucha importancia introducir headers (cabeceras) en los correos para mejorar su entregabilidad. Un header es una cabecera que el usuario normal lector de un correo no ve pero que los proveedores de correo pueden usar. Estos headers relacionados con listas se definen en el RFC 2369. Este aspecto podría necesitar la ayuda de un programador o un técnico especializado para su establecimiento, si la herramienta que se está usando no la implementa de una manera accesible.

Se define en primera instancia el header **List-Help**, que define una dirección web o email en el que solicitar u obtener ayuda sobre la lista.

El más importante de estos headers es **List-Unsubscribe**. Estableciendo este header le damos al usuario la posibilidad de desuscribirse rápidamente debido a que los grandes proveedores le mostrarán un enlace en el correo para realizar la desuscripción. Puede ser un correo o bien una dirección web de baja automática. Por ejemplo Google muestra el enlace del siguiente modo:



Hay otras cabeceras definidas, pero las anteriores son las más usadas. Los grandes proveedores puntúan positivamente a aquellos usuarios que envían boletines que incluyen estas cabeceras.

Software para envío de boletines

La elección del software para el envío de boletines siempre debe ser una elección importante en el proceso de generación de listas de envío. Hay mucho software que se ocupa de las tareas anteriormene descritas de modo automático (delistado automático de direcciones fallidas, delistado de peticiones de usuarios, etc.). Aquí en guebs.com se dispone de mailman de serie en todos nuestros servicios y disponemos de algunas guías para usar software común. Mailman es un software

longevo y que dispone de todas las características que se han descrito en esta guía, pero tiene una curva de aprendizaje algo alta. Hay otros softwares más sencillos de los cuales detallamos algunos a continuación.

Para usar phplist:

Como usar phpList para enviar Newsletter

Si quieres usar tu propio programa de correo, es necesario que lo hagas siguiendo las directrices indicadas: un correo por usuario, gestión de listas y rebotes, etc. Hay algunos plugins disponibles que te pueden ayudar a gestionar estas listas

Como enviar boletines de forma fácil con Outlook y Send Personally

Baja frecuencia de envío

Hay proveedores que tienen medidas de tolerancia muy bajas. Por ejemplo la baja frecuencia de envío en servidores dedicados o en ips recién añadidas a servicios dedicados en marcha puede provocar que ese proveedor marque tu correo como poco fiable. Se trata del concepto de 'calentar' una ip.

Autenticación de correo

Aquí en guebs.com todos los dominios que alojamos disponen de registros SPF, DKIM y DMARC, pero deben ser revisados si encuentras problemas con tu correo electrónico.

Como activar DKIM y SPF en tu correo electronico

Usar software actualizado

Los problemas por usar software obsoleto son muchos. En primer lugar por los problemas de seguridad que su uso conlleva. Además estos programas ya no están adaptados para las necesidades actuales y algunos de ellos pueden incluso generar correo malformado.

Envío de correos desde una aplicación web

Es muy común que los correos que se envían desde una web acaben en spam. La causa consiste en que es más sencillo despistarse en relación a los aspectos más comunes. Éstas son las causas más comunes que debes revisar cuando configuras tu aplicación web para el envío de correos.

– La dirección «from:» desde la que envías desde tu aplicación web tiene que ser una dirección de tu propio dominio. No uses una dirección de gmail, hotmail, o cualquier proveedor que no sea tu dominio: no funcionará . Muchos usuarios instalan un cms cualquiera y establecen direcciones de hotmail o gmail como remitentes. Éste es el primer punto que se debe examinar.

– Conviene que, si tu software lo soporta, uses autenticación smtp. Esto mejora la entregabilidad de tu correo enviado desde la web. Para wordpress por ejemplo:

Cómo mejorar el envió de correo en WordPress con Easy WP SMTP

– Hoy en día, si tu aplicación presenta formularios de contacto, éstos deben ser protegidos adecuadamente. Su abuso es común y creciente. Por ello, los formularios de contacto tienen que ser protegidos con algún tipo de captcha:

https://es.wikipedia.org/wiki/Captcha

Es muy común usar contact-form en wordpress. Para detener el spam que llega de este plugin, se puede aplicar una medida simple como la siguiente:

Añadir protección AntiSpam con el plugin Contact Form 7

Desde hace mucho tiempo google ofrece el servicio de recaptcha, que resultará útil para muchos desarrolladores web:

https://www.google.com/recaptcha/intro/v3.html

Para integrar recaptcha en wordpress de modo global, se puede consultar la siguiente guía:

Protege los formularios de WordPress con reCAPTCHA

Codificación de los correos

Este aspecto corresponde especialmente a aquellos usuarios que elaboran sus propios correos desde una aplicación web (desarrolladores, webmásters, etc.). Un analizador anti-spam no ve el correo como lo ve un humano, sino que escanea el mismo en función de cosas que 'hay' y cosas que 'no hay'. Por ello, conviene evitar aspectos comunes que muchos correos tipificados como spam cumplen. Por ejemplo:

– Si envías tu correo en formato html, entonces el correo debe tener una alternativa en texto plano.

– Si envías tu correo codificado en base64, entonces las probabilidades de que sea considerado spam es mayor.