



WebHosting al mejor precio y con la mayor calidad

Manual de cómo evitar que mi correo sea catalogado como SPAM

El concepto de SPAM todo el mundo que tiene y utiliza el correo electrónico lo conoce y sabemos lo molesto que resulta para nuestro ocio o para nuestro trabajo diario, pero más molesto aún es que las empresas vean cómo sus correos publicitarios o comerciales por algún misterioso motivo son catalogados como SPAM y no llegan a sus clientes - destinatarios.

Para evitar este problema vamos a explicar que es lo que hay que realizar para evitar esta desagradable situación. Pero antes de comenzar hay que señalar que el sistema de WebHosting puede ser compartido y esto significa, que varios dominios utilizan la misma IP y el mismo Servidor para distintos alojamientos de Correo y de Web, por lo tanto, puede ocurrir que ciertas empresas de correo con sus diferentes sistemas AntiSpam coloquen la IP como 'sancionada'. Aunque nosotros hagamos un correcto uso de nuestro correo y sigamos todos los consejos e indicaciones aquí descritos es posible que sigamos teniendo este contratiempo. Para solucionar este problema tendremos que buscar una alternativa mucho más costosa que es adquirir un sistema de Hosting Privado asignándose nuestra propia dirección IP fija para nuestros dominios y así evitamos que otros usuarios menos responsables hagan lo que no tienen que hacer.

Los principales motivos por los que sus correos pueden ser detectados como SPAM:

.Los destinatarios de su correo no quieren recibirlo o no son capaces de visualizarlo correctamente y realizan una denuncia de SPAM en las listas RBL (listas negras publicas internacionales).

.Su correo es detectado automáticamente como SPAM por los filtros Bayesianos.

Para evitar que sus correos sean catalogados como SPAM siga estos pasos:

1. Revise las Direcciones de los E-Mails de envíos.
Compruebe que los correos que envía tiene todas las direcciones correctas y evite entregar correo a persona no deseadas e inexistentes. Actualice esas direcciones.
2. Realice buenas prácticas sobre el permiso de sus clientes u futuros clientes.
Si tiene un sistema de suscripciones manténgalo actualizado y permita que los suscriptores puedan darse de baja en el servicio de una forma clara y sencilla.
3. Infórmese de su ISP de su servidor de Correo.
Si su ISP ha sido denunciado a una blacklist, los correos que envía a través de sus servidores serán catalogados como SPAM.
4. Revise el Subject y el Cuerpo de sus correos sobre todo si los realiza en HTML.
Por ejemplo no escriba todo el Subject en Mayúsculas, no reitere muchos símbolos en su mensaje y no escriba repetidas veces palabras como *Free* o *Gratis*, *Click aquí*, ... Sea también cuidadoso con su código HTML.
5. Configure correctamente la opción *Email Authentication* en su Panel de Control *CPanel*.
Tras comprobar que su servidor tiene activo la resolución inversa de DNS, dentro de la sección Correo en su *CPanel* tenemos la opción *Email Authentication* y debemos de activar la opción de *DomainKeys* y *SPF*. La activación de *DomainKeys* es muy sencilla ya que se realiza automáticamente en el botón correspondiente.
Y para activar *SPF* debe rellenar también las configuraciones avanzadas de :
'Hosts Adicionales que envían correo para sus dominios (A)' con su nombre de servidor.
'Bloques de IP adicionales para sus dominios (IP4)' con la IP de su servidor.
Y señale la opción de 'Sobrescribir Datos Existentes'.

Si tiene alguna duda puede consultarnos directamente para indicarle el nombre de su servidor o IP y si lo desea el equipo de *Soporte Técnico Vigunu* puede configurarlo directamente.

Vea las imágenes como quedaría.

**Email Authentication**

La autenticación de correo es el esfuerzo para equipar mensajes del sistema de transportación del correo con suficiente información verificable, de esta manera los recipientes pueden reconocer la naturaleza de cada uno de los mensajes recibidos automáticamente.

DomainKeys

DomainKeys es un sistema de autenticación de correo diseñado para verificar el dominio de DNS del envió del correo y la integridad del mensaje. La especificación de DomainKeys ha adoptado aspectos de Identified Internet Mail para crear un protocolo mejorado llamado DomainKeys Identified Mail (DKIM).

Status: Activado & Activo (Chequeo de DNS Paso la Prueba) [Desactivar](#)

SPF

SPF permite que el software pueda identificar y rechazar direcciones forjadas en el SMTP MAIL FROM (Return-Path), algo típico en lo referente a spam de correo.

Status: Activado & Activo (Chequeo de DNS Paso la Prueba)

[Desactivar](#)

Your current raw SPF record is : **v=spf1 a mx ip4:** Ip de servidor **a:** Nombre de Servidor **?all**

Configuraciones Avanzadas:**Hosts Adicionales que envían correo para sus dominios (A):**

[Crear](#)

[Borrar](#)

Todos los hosts que especifique aquí serán aprobados para enviar correo. No necesita especificar su mail exchanger primario o cualquier servidor para el cual ya ha sido creado un récord mx ya que están incluidos automáticamente.

Nombre de Servidor

Servidores MX adicionales para sus dominios (MX):

[Crear](#)

[Borrar](#)

Todos los datos de mx para cada dominio que especifique aquí serán aprobados para enviar correo.

Bloques de IP adicionales para sus dominios (IP4):

[Crear](#)

[Borrar](#)

Todos los bloques de IP que especifique aquí serán aprobados para enviar correo. Los bloques deben de ser especificados en formato CIDR (por ejemplo ie 127.0.0.1/32).

Ip de Servidor

The main server interface ip cannot be removed from this list if it is present. The following ip is the main server interface ip:

Lista de Inclusión (INCLUDE):

[Crear](#)

[Borrar](#)

Las configuraciones SPF para todos los hosts que especifique en esta lista serán incluidas con sus configuraciones de SPF. Esto es beneficioso si va a enviar correo mediante otro servicio. (ex. mac.com, comcast.com, etc).

Todos los Datos (ALL):

Si esta seguro de que puso todos los hosts (su mail exchanger primario y cualquier otro dato mx son incluidos automáticamente) que enviaran correo de tu dominio, seleccione esta caja para excluir cualquier otro dominio.

Sobrescribir Datos Existentes:

Si selecciona esta opción todos los records de spf existentes serán sobrescritos para todos sus dominios con esas selecciones.

Salvar Sus Cambios:

[Actualizar](#)

Guarde los cambios dando al botón 'Actualizar'.

6. Nunca haga SPAM.
El envío masivo e indiscriminado de Emails (Mailing) a personas que no los han solicitado, por experiencia, no le hará aumentar sus ventas. Al realizar esta práctica dañara la imagen de su empresa y tarde o temprano acabará originándole serios problemas.
7. Lea con detenimiento los términos y condiciones de Vigunu para conocer las actividades y contenidos que no están permitidos en nuestros servidores.

Para obtener mas información sobre SPAM :

<http://es.wikipedia.org/wiki/Spam>

