Cómo filtrar el correo basura spam dejando llegar bien solamente los mensajes deseados?

6 tips para hacer llegar correctamente a la bandeja de entrada únicamente a los emails correctos

Si hay una preocupación diaria de cualquier usuario de casilla de email personal, es: "todo email correcto lo quiero llegando a mi bandeja de entrada siempre y todo email basura quiero que no me llegue, o sino al menos que llegue a la carpeta de *SPAM* sin contaminar la bandeja principal".
Este deseo puede hacerse realidad, pero el 100% de eficacia en este objetivo implicará dedicar algo de tiempo, aprendizaje, y sobre todo un proveedor de servidor de email

que pueda brindar el funcionamiento ideal, y tambien orientar al usuario final con los consejos correctos.
En esta nota proveemos información específica para entender un poco más cómo resolver este tema para siempre.

Dividiremos los tips en 2 grupos: 3 tips de naturaleza ténica y de servicio, los cuales suelen ser responsabilidad del proveedor de tecnología de la solución de mailing, y 3 tips de prácticas de uso, los cuales están dirigidos al usuario final que opera la cuenta de email.

A grandes rasgos, como se logra filtrar sólo el correo basura sin afectar al correo deseado?

Desde que el email se empezó a utilizar en todo el mundo como medio de comunicación, fue creciendo exponencialmente el correo basura, y como reacción a esto, también fue creciendo el uso a veces excesivo de programas, plataformas y reglas anti-spam.
En muchos casos al recibir cada mensaje, saber si se trata de correo basura es algo sencillo para la mayoría de los sistemas, pero tambien son muchos los casos en que se fue tornando cada vez más dificil discriminar con eficacia y exactitud qué correo es realmente spam y qué correo es un correo válido para recibir.
Por eso creemos que para resolver este problema, además del sistema provisto de base por el proveedor, se necesitarán algunos conceptos adicionales para que el usuario pueda dominar el tema sin complicarse en el intento.

Como parte del servidor de email existirán siempre algunos filtros de base, los cuales no deben ser excesivos, para nunca poner en riesgo la llegada de emails válidos. Como

complemento a estos filtros, serán necesarias algunas tareas del usuario final para así asegurar el funcionamiento ideal.

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten aplicar y revisar toda esta información en detalle, y tener configurado el SERVIDOR DE EMAIL de acuerdo a lo necesario para asegurar lo recien mencionado. Consúltenos para así obtener información actualizada sobre nuestros planes:

Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda	**5411 47982212** (lun/vie 10/19 hs)	**54911 54594979** (lun/vie 10/19 hs)

A CONTINUACIÓN DESARROLLAMOS LOS 6 TIPS

TIPS TÉCNICOS Y DE SERVICIO DEL PROVEEDOR

Estan orientados a ser cumplidos por los proveedores de servidores y soluciones de mailing. Cuando el usuario final recibe las credenciales para acceder a un panel, usar su casilla de email, utilizar su webmail y/o programa tipo Outlook, estos puntos ya deberían estar funcionando por parte de quien ofrece la solución.

1. CONFIGURACION DE FILTROS DE BASE EN EL SERVIDOR SMTP

Los servidores de email que se asignan a un dominio como el caso de Postfix, Exim, Exchange, y otros, permiten establecer reglas y configuraciones de base que hoy en día son fundamentales, y deberán estar siempre correctamente aplicadas, aquí enumeramos algunas de las más importantes:

- Que el MX del servidor no sea un OPEN RELAY (o sea que no pueda ser reusado externa ni remotamente por otro usuario o dominio)
- Que se soporten conexiones TLS y SSL para permitir encripción de mensajes y datos
- Los correos que entren o salgan sólo podrán aceptarse si estan autenticados por usuario (email) y contraseña de una cuenta de email de dominio. Cuando esto no se cumple, se generan rechazos automáticos
- Los correos que se reciban pertenecerán a un dominio válido online. Cuando esto no se cumple, se generan rechazos automáticos
- Aplicación de filtros por LISTA NEGRA. En esta instancia sólo recomendamos:
    - Rechazar correos que tienen como origen una dirección IP listada en SPAMHAUS (100% recomendado)
    - Rechazar correos que tienen como origen una dirección IP listada en SPAMCOP (100% recomendado)
    - Rechazar correos que tienen como origen una dirección IP listada en SORBS SPAM (decisión sujeta al administrador de email)

  Aclaración importante: Cuando se suman listas negras de menor relevancia, es muy habitual que los usuarios pasan a no recibir mensajes de contactos bien intencionados, por eso insistimos en no sobrepsarse con los filtros de base a aplicar.

2. SERVER-SIDE: FIREWALL, ANTISPAMS, PANEL DE AUTOGESTIÓN Y WEBMAIL

El servidor de email debería estar en un entorno de red protegido. Para ello será necesaria la existencia de un **FIREWALL**, el cual actuará para evitar intrusión en el servidor a nivel general, y algunas de las reglas de cualquier firewall benefician a la salud del sistema de emails. Por ejemplo: al ir creando listas de ips a rechazar, esos intentos remotos tampoco afectarán al sistema de cuentas de email.
Algunos ejemplos recomendables: CSF FIREWALL, o FAIL2BAN

Tambien en la nube podrá optarse por activar un **ANTISPAM** que ayude a gestionar criterios y reglas anti-spam del lado del servidor. Respecto a este punto, recomendamos cautela en las configuraciones, ya que un anti-spam excesivo podría crear problemas al no recibir emails que se deseaban recibir.
Algunos ejemplos: CLAMAV, SPAM ASSASIN

Otra herramienta importante es el **PANEL DE AUTOGESTIÓN DE CUENTAS**. Este panel permitirá que un usuario administrador pueda: crear cuentas, contraseñas, eliminar cuentas,

aplicar autorespondedores, y lo más importante en referencia a este tema: APLICAR FILTROS tanto a nivel general, como a nivel de cuentas individuales. (desarrollado en el punto 5)

Y finalmente, la herramienta más utilizada por el usuario final: el **WEBMAIL** que reside junto al servidor de email, y es mediante la cual el usuario final podrá ir aplicando filtros del mejor modo posible, ya que los filtros que residan en su programa de email de pc actuan en cierta manera tarde, cuando el correo ya llegó a su pc.
Algunos ejemplos: ROUNDCUBE (más habitual), HORDE, SQUIRRELMAIL

3. ORIENTACIÓN AL USUARIO FINAL DESDE EL DÍA 1

En **webmatter** consideramos que una vez configurado el entorno del lado del servidor, la razón principal para resolver el tema de esta nota, es la orientación que damos a los usuarios para que operen correctamente desde los primeros días, dominando el tema de criterios y filtros anti-spam.
Esto va generando una historia positiva en el manejo de contactos y mensajes, lo que finalmente termina logrando una calidad en la operación al recibir sólo los mensajes útiles en la bandeja de entrada, y por otro lado no recibir más spam.

TIPS PARA EL USUARIO FINAL

Estan orientados a ser cumplidos por la o las personas que operarán casillas de email, o a usuarios administradores que tengan como responsabilidad gestionar cuentas de email de un grupo de personas. De acuerdo a nuestra expereiencia, una vez que transmitimos estos conceptos al comienzo, sumado al servidor de email correctamente configurado, el problema del correo basura suele solucionarse sin inconvenientes.

4. EXISTENCIA DE UNA *LISTA BLANCA* DE CONTACTOS Y DOMINIOS

El primer punto a considerar será tener siempre actualizada una AGENDA DE CONTACTOS, similar a lo que sucuede con el teléfono celular.
Cada dirección de email debería existir en dicha agenda. Hay más de una opción para el mantenimiento y gestión de esta lista:

- Agenda de contactos en la nube: en programa WEBMAIL se podrá ir actualizando esta lista, en un tratamiento idéntico al que sería la gestión de una lista de contactos en GMAIL, HOTMAIL, etc
  Lo ideal es asegurarse que cada contacto de la agenda, además existe en la sección de filtros en la parte de REMITENTES SEGUROS y que su dominio existe en la parte de DOMINIOS SEGUROS de dicho filtro.
- Agenda de contactos en programa de pc como OUTLOOK o THUNDERBIRD: En un tratamiento similar, podré hacer lo mismo en la pc, con la diferencia, como dijimos antes, que en la pc está llegando todo lo que no fue filtrado en la instancia de servidor, como el caso del webmail. La ventaja de utilizar un programa de pc, siempre y cuando el tipo de conexión al servidor sea POP3, será que se tendrá en todo momento un resguardo personal de toda la información: de contactos, mensajes, reglas de filtros, etc.

Una vez que se incorpora esta idea al día a día del usuario, se podrá luego pasar a dominar este tipo de listas de contactos y direcciones de email: permiten resguardarse, exportarse en excel, importarse, etc etc.
El resguardo periódico de este tipo de listas o agendas, asegurará el hecho de nunca perder lo recorrido a través del tiempo: estamos hablando de información sensible, importante para cualquier necesidad y contexto. Recomendamos al menos 1 vez por mes resguardar la información en un dispositivo usb, como el caso de un disco rígido externo o pen drive, y/o en un espacio en la nube.

5. AUTOGESTIÓN DE FILTROS (MUY IMPORTANTE)

Al momento de recibir cada correo basura, se debería tomar una medida que ayude a que eso no ocurra en el futuro.
Para que sea más claro, daremos un par de ejemplos:

1. Supongamos que se trata de un correo basura aislado. En ese caso, lo ideal es: En programa de pc como OUTLOOK, aplicar boton derecho del mouse, y seleccionar las opciones para considerar al correo *no deseado*, bloquear el remitente, y asegurarme que fue movido a la bandeja de correo no deseado.
   En el WEBMAIL de la cuenta de email, en la sección de FILTROS, agregar el dominio

origen de ese mensaje a la lista de dominios a bloquear
Luego de esto, se podría eliminar el mensaje de Outlook

2. Supongamos que se recibieron múltiples correos similares o iguales, a modo de ataque spam (VIRUS):
   En un caso así la primera acción debería ser comunicar el caso al proveedor de servidor de email, ya que podría ser un virus de gravedad, y lo ideal es actuar lo antes posible para detenerlo.
   Luego de esto, el procedimiento del lado del usuario final es sencillo: agregar el dominio origen de esos emails en la lista de dominios a filtrar del webmail, y luego eliminar todos los mensajes que se habían recibido, asegurandose de que no vuelva a llegar otro mensajes despues de esa instancia.
   Obviamente este caso implicará mantener contacto con el proveedor de servidor, hasta que el mismo indique que el problema fue normalizado. Se debería renovar la contraseña de la cuenta de email, como una medida de seguridad preventiva.

6. SEGURIDAD Y PREVENCIÓN (MUY IMPORTANTE 2)

Existen algunas sanas costumbres para el uso del email, que tambien terminarían beneficiándo la operación del usuario a futuro:

- Utilizar unicamente CONTRASEÑAS SEGURAS. La época de la clave *pepe123* caducó hace años, hoy en día las contraseñas deben tener más de 10 caracteres, incluir mayúsculas, minúsculas, números y caracteres especiales
- Coordinar con el proveedor de servioio de email, el hecho de que cualquier intento de pedido de dato confidencial, login no programado, url de panel, etc, no podrá ocurrir via email a menos de que asi haya sido acordado previamente. El fishing es uno de los típicos modos de fraude hoy en día.
- Siempre tener un resguardo periódico de toda la información: contactos, mensajes, etc (antes mencionado)
- Operar de forma ordenada los emails: crear subcarpetas, eliminar lo que no sirva, etc
- Administrar de forma ordenada los contactos: mantener sus datos actualizados, eliminar lo que no sirva, etc
- Tener aplicados los puntos 1 a 5 de esta nota para la correcta operación de emails

Esperamos que esta nota te haya resultado útil!
Para más información detallada, aguardamos tu contacto.

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten aplicar y revisar toda esta información en detalle, y tener configurado el SERVIDOR DE EMAIL de acuerdo a lo necesario para asegurar lo recien mencionado.
Consúltenos para así obtener información actualizada sobre nuestros planes:

Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda en https://web-matter.com.ar	**5411 47982212** (lun/vie 10/19 hs)	**54911 54594979** (lun/vie 10/19 hs)