Protocolo de Seguridad en Internet

Internet no es un medio seguro. Desvelamos más información acerca de nosotros mismos de lo que imaginamos. Somos víctimas fáciles de asaltos a la intimidad como el *spam*, la suplantación de identidad o el marketing personalizado. Cada vez que navegamos, dejamos un rastro fácil de seguir. ¿Es el fin de la intimidad?

Ante los posibles ataques de virus, troyanos, spam y otros elementos que pueden infectarnos, es imprescindible dotar a nuestro sistema de ciertos programas que vacunan, inmunizan y lo protegen al tiempo que atacan posibles códigos nocivos presentes en nuestro PC y cumplir un **Protocolo de Seguridad (Activa y Pasiva) en Internet.**

Qué es un Virus Informático??

Un **virus informático** es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM del PC, aun cuando el programa que lo contenía haya terminado de ejecutarse.

El virus toma entonces el control de los servicios básicos del sistema operativo, infectando archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Qué es un Troyano?

Se denomina **troyano** (o *caballo de Troya*) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona, pero sin afectar al funcionamiento de ésta.

Un troyano no es de por sí, un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal.

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo del ordenador hace y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado y dotado de buena heurística. Es recomendable también instalar algún software anti troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un firewall.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

Los troyanos están actualmente ilegalizados, pero hay muchos crackers que lo utilizan.

Diferencias entre un virus y un troyano?

La diferencia fundamental entre un troyano y un virus consiste en su **finalidad**. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina infectada sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano evita provocar daños porque no es su objetivo.

El Spam....

El término “Spam” (Spiced Ham), se utilizaba para aludir a la carne enlatada que se proporcionaba a los soldados americanos. Debido a su pobre calidad, se ganó una fama totalmente negativa.

Se denomina correo basura (en inglés también conocido como *junk-mail* o *spam*) a una cierta forma de inundar la Internet con muchas copias (incluso millones) del mismo mensaje, en un intento por alcanzar a gente que de otra forma nunca accedería a recibirlo y menos a leerlo. La mayor parte del correo basura está constituido por anuncios comerciales, normalmente de productos dudosos, métodos para hacerse rico o servicios en la frontera de la legalidad. No deja de amargar la existencia a los usuarios de Internet cuando encuentran sus buzones rebosando.

Las listas de correo basura con las direcciones de correo electrónico de los clientes potenciales (o víctimas seguras) se crean frecuentemente cribando los mensajes de Usenet, robando direcciones en las listas de distribución o comprándolas en las bases de datos de los servicios en línea de Internet o bien buscando direcciones por la red. Irónicamente, los propios spammers usan el spam para anunciarse.

En qué consiste el Protocolo de Seguridad para Internet??

Es un conjunto de sencillos pero importantes pasos que nos ayudará a mantener nuestro sistema alejado de los virus, troyanos, gusanos, spam....

El primer paso es conseguir una copia de los programas necesarios para proteger nuestro sistema: Son básicamente cinco:

1.- Avast Antivirus: Antivirus residente y auto actualizable.

2.- CleanUp!: Herramienta que **libera** nuestro sistema de los archivos temporales que ocupan espacio en nuestro disco duro y proporcionan "escondite" a virus y troyanos.

3.- SpywareBlaster: esta aplicación es equivalente a **Seguridad Pasiva**, **vacuna** nuestro PC ante posibles contagios.

4.- Spybot Search and Destroy: Seguridad Activa y Pasiva, vacuna nuestro PC y **ataca** a posibles códigos nocivos instalados ya en nuestro sistema.

5.- Filtro AntiSpam: Filtro adaptativo que analiza nuestro buzón de entrada, clasificando y señalando los posibles Spams. Es configurable por el usuario. Incluye además un filtro Antivirus.

Contáctenos y le instalaremos una copia.

Los clientes que tienen un dominio alojado en el servidor de Redesna disponen un Filtro AntiSpam ya instalado para todas las direcciones de correo asociadas al dominio.

Una vez instalados las otras cuatro aplicaciones en su PC hay que tener en cuenta una gran diferencia entre ellas:

El **Avast Antivirus** es un antivirus **residente** que se **actualiza automáticamente**, es decir, una vez instalado está siempre vigilando nuestro ordenador y se actualiza descargando las novedades de Internet sin necesidad de que hagamos nada. Tan sólo

es necesario renovar la licencia, una vez al año. Para usos puntuales dispone de un manual del Avast Antivirus en nuestro área de clientes.

A diferencia de esta herramienta residente, el resto de aplicaciones requieren ejecución y configuración manual.

El filtro AntiSpam ha de configurarlo una sola vez y después, si es necesario, aplicarle retoques según sean los resultados.

Las otras tres aplicaciones (CleanUp!, SpywareBlaster y Spybot) han de **ejecutarse y actualizarse manualmente una vez a la semana**. Requiere un esfuerzo por su parte, pero si adapta esta costumbre en sus hábitos, no sólo mantendrá su PC alejado de los virus, sino que lo mantendrá en óptimas condiciones evitando que se acumulen archivos inútiles en carpetas ocultas y que relenticen el rendimiento de su sistema, evitando así pérdidas de tiempo.

El orden de los pasos también es importante: primero tener siempre activado el avast antivirus y después una vez a la semana ejecutar primero el CleanUp!, después el SpywareBlaster y por último el Spybot Search and Destroy. Para ello consulte nuestros manuales correspondientes en el área destinada a nuestros clientes.

Por último, pero no menos importante es tener instalado un filtro AntiSpam que minimice la posibilidad de que llegue a nuestro buzón posibles ataques en forma de mail ó archivo adjunto.

Los clientes que dispongan de un dominio alojado en el servidor de Redesna Informática S.L. disponen desde finales del 2006 de un filtro AntiSpam adaptativo, es decir es un filtro que analiza todos los mensajes recibidos y “aprende” a distinguir entre el Spam y los correos reales. No hay sistema infalible por lo que es recomendable que sintonice el filtro según sus necesidades y la respuesta del sistema. Para ello consulte nuestro manual AntiSpam en el área destinada a nuestros clientes.

RECUERDE:

Solicítenos la instalación de una copia del **Avast Antivirus** y déjelo trabajar como residente en su sistema. Permita que se actualice manteniendo el PC conectado a Internet.

Solicítenos la instalación de una copia del **Software AntiSpyware** (CleanUp!, SpywareBlaster y Spybot), **actualice y ejecútelos una vez por semana.**

Dote su cuenta de correo de un **filtro AntiSpam** moderno y efectivo que mantenga el Spam a raya.

Estas tres costumbres y algunas precauciones son más que suficientes para mantener su sistema inmune.

A continuación se incluyen artículos de interés sobre virus, troyanos y Spam: como llegan a nosotros, por qué es malo y qué podemos hacer para evitarlo. Disfrute de la lectura !!!

Virus, troyanos, gusanos y spam: Échale la culpa a Marte

Marte: dios de la guerra, dice la mitología clásica que cada vez que ese planeta se aproxima al nuestro, aumenta nuestra belicosidad.

Sin embargo y tal vez para darle más letra a la literatura, la comunidad de Internet se ha visto invadida por virus, troyanos, gusanos y cuanto bicho puede afectar un ordenador, sin olvidar el último elemento que se apunta a la lista de ataques informáticos: el spam (o correo no solicitado) que parece ser uno de los “bichos” más poderosos, no por dañinos en sí mismo, sino por la pérdida de productividad que trae aparejada el deshacerse de toda esa basura.

Cómo llegan a nosotros??

La gran mayoría de los virus, troyanos y gusanos que andan por la Red llegan a nuestro ordenador adjuntos a un e-mail. Al hacer doble clic sobre ese adjunto lo que hacemos, sin saberlo, es ordenarle al sistema operativo que ejecute el código que contiene, en otras palabras, lo pone a trabajar en nuestro PC, en tareas “non sanctas”, obvio.

De ahí que la mejor precaución sea sencillamente no darle doble clic a ningún adjunto sospechoso que llegue en un mensaje de correo electrónico. Nunca!!!

Lo más conveniente es eliminar el mensaje con el archivo adjunto y olvidarse del problema.

Como protocolo de seguridad ante mensajes con adjuntos de remitentes conocidos, lo más conveniente es guardarlo en nuestro PC, aunque sea en el escritorio y revisarlo con un antivirus actualizado antes de abrirlo.

Lo que nos lleva al siguiente consejo: los **antivirus deben estar actualizados**, porque lamentablemente virus nuevos y variaciones de los mismos (¿nuevas cepas?) aparecen todos los días.

Las indicaciones de pasar un antivirus actualizado antes de abrir un archivo, se aplican también a los archivos que bajamos de Internet, no solamente a los adjuntos de correo.

Volvamos un paso atrás ¿hace falta bajar el adjunto, pasar el antivirus, etc, etc con cada archivo adjunto?

Noooo, cuando se llega a recibir 200 o 300 emails diarios y 90% no sirven para nada, a golpes se aprende a detectar el olorcito del spam.

Contengan o no contengan virus no hace falta ser adivino para, sin abrir siquiera el mail, reconocer algunas “joyitas” destinadas a la papelera.

Puede pulsar el botón **borrar** sin cargos de conciencia cuando el asunto es:

- The most profitable business
- enlarge your pennis (con simple o doble "n", la estrategia de las faltas de ortografía son para burlar los filtros)
- please reply
- Los que vienen todos con signos en chino o coreano o no se que... (¿lee esos idiomas? ¿entonces para qué abrirlos?)
- became millonaire now (siga trabajando, no pierde nada)
- Hi y sus variedades hola, etc, etc
- lo que me preguntaste (y si, uno/a cae como un/a tonto/a)
- Free gift offerings
- Cuando quien lo envía es usted mismo/a o una variación sutil de su dirección de email (astutos.....)
- Cuando el remitente tiene un email xhyyy23hy67sj@hotmail (¿alguien tendría un email así?)
- Get out of debs for free (ah, sí suena bien …)
- Viagra, no prescription needed
- Your $7500 Platinum card is waiting (que siga esperando….)
- Cuando el remitente es el Sr. Mobutu o variaciones de la misma estafa nigeriana (algun día analizaremos el caso...)
- Hot girls...
- Si el archivo tiene doble extensión (ejempo: doc.pif)

Paremos aquí, ¿los documentos que recibe no tienen extensión? Este tipo de archivos ha sido siempre característico de los sistemas operativos de Mac, sin embargo, dependiendo de su configuración, hace tiempo que los PCs también leen archivos sin extensión.

Para ahorrar tiempo le conviene activar la opción mostrar extensiones. En cualquier carpeta abierta vaya a Tools (Herramientas)>Folder Options (Opciones de carpeta) > View (ver) allí quítele la tilde a Ocultar extensiones para los tipos de archivos conocidos. Listo ahora podrá ver las extensiones, las válidas y las otras.

Usted se preguntará si con esta metodología de limpieza indiscriminada no pierdo algún correo útil, y sí , pero le recuerdo: no hay empresa sin riesgos...

Cada vez es más importante desarrollar cierta capacidad de evaluar lo que viene en el campo Asunto, pues es justamente ahí donde se libra la primera batalla. ¿qué batalla? La de entrar en su sistema.....

Quien quiera entrar a su PC (ya sea sólo para molestar o para tratar de sacar información) tiene que tentarla/o con el mensaje, en definitiva, las técnicas de seducción están a la orden del día. De la misma manera, piense bien lo que va a escribir en el Asunto de su email, ya sea que se dirija a una persona conocida o no, su email puede ser muy válido y valioso pero, si en vez de abrirlo, lo borran de entrada...

Por qué es malo el SPAM ???

En primer lugar, porque nos cuesta tiempo y dinero. Para aquellos que se conectan vía telefónica, los pasos siguen corriendo mientras se lee o recibe su correo, lo cual, al recibir montones de basura, les cuesta un dinero adicional.

A un nivel superior, a los proveedores de Internet y a los servicios en línea les cuesta dinero el transmitir el correo basura, coste que se añadirá posteriormente a la cuota de sus suscriptores. Una estrategia especialmente deplorable consiste en conseguir durante unos días una cuenta de prueba de un proveedor de Internet, enviar miles, millones de mensajes, y abandonar la cuenta, dejando al proveedor empantanado.

El correo basura, como su nombre indica, es basura. ¿Y a quién le interesa recibir basura en su buzón? La inmensa mayoría de los correos basura que son indiscriminadamente enviados por la Red casi sin excepción anuncian géneros sin el más mínimo valor, engañosos y más o menos fraudulentos.

Desde software para enviar correos basura (autopromoción, ¿no?), dietas y curas milagrosas, a componentes sin marca de ordenadores, desde misteriosos métodos para hacerse rico en unos días, a sitios pornográficos, y de ahí a peor. Se trata de material demasiado impresentable como para anunciarlo en medios respetables donde deberían pagar por anunciarse.

Los spammers (los que envían correo basura) son gentes sin escrúpulos, que no tienen reparos en congestionar servicios de acceso a Internet, como ocurrió con America On Line, que se dice

llegó a recibir 1,8 millones de correos basura al día de CyberPromotions. Suponiendo que una persona emplee diez segundos en identificar y descartar de su buzón un correo como basura, significaría que se desperdiciarían 5.000 horas de tiempo de conexión por día simplemente para deshacerse de esos correos, y sólo en AOL.

Sumemos el tiempo de conexión en toda la Red. **Nada en el mundo cuesta tan poco al anunciante y tanto al destinatario.**

Además, en muchas ocasiones los contenidos rozan la ilegalidad, si es que no son manifiestamente ilegales, como la pornografía infantil.

Cómo evitarlo ?

Ésta es una cuestión peliaguda, ya que, estrictamente hablando, no existe forma humana (ni mecánica) de evitarlo por completo. Se pueden apuntar una serie de sugerencias, que si bien no nos impermeabilizarán al correo basura, sí que al menos lo harán disminuir significativamente.

La prevención esla mejor manera de evitar que su correo aparezca en las listas de spammer. Conocer como funcionan es el primer paso para plantarle batalla.

Uno de las principales fuentes de las que obtienen direcciones de correo es la captura por software automático de miles y miles de direcciones diarias que figuran en las páginas web como contactos para clientes. Una vez que la dirección email comienza a circular cada vez integra mayor cantidad de listas “públicas”.

Existen robots que buscan direcciones de correo por las páginas de Internet. Para frustrar sus esfuerzos, se puede incluir la dirección de correo en una imagen, en formato gif o jpg, de manera que cualquier lector humano sea capaz de reconocerla, mientras que les pasará inadvertida a los robots automáticos.

Otra manera de presentar su contacto en Internet de manera que su dirección no sea susceptible de ser capturada por los robots automáticos es a través de formularios.

Reemplace su dirección de correo a la vista por un formulario de contacto. Dicho formulario se programa de forma tal que dependiendo del asunto de contacto, se envía al email a la persona encargada. Pero el email, no sólo no está a la vista sino que no puede ser capturado por uno de estos programas automáticos.

Cuando en alguna página en particular no se puede poner dicho formulario, entonces lo codificamos. El email está allí, funciona, pero no es legible.

De esta manera, a pesar de que cuando pasa el ratón sobre el enlace se ve claramente la dirección, los spammers no captan los mails de esa manera.

Ésto es lo que el programa que recoge mails ve en la parte correspondiente a la dirección de correo:

```
<script type="text/javascript"> // <!--[CDATA[ < !-- var x="function
f(x){var i,o=\"\",ol=x.length,l=ol;while(x.charCodeAt(l/13)!" + "
=50){try{x+=x;l+=l;}catch(e){}}for(i=l-1;i>=0;i--
){o+=x.charAt(i);}return o" + "
.substr(0,ol);}f(\")25,\\\"IAKFLSr\\\\DVX]--
>79230\\\\hw010\\\\bgb410\\\\\\\"\\\\;>}~y520\\\\:g4$ -
#410\\\\bc300\\\\"+ "
XPOSM030\\\\520\\\\j330\\\\b530\\\\q410\\\\DLKGN^Y620\\\\ZF01
0\\\\HK@410\\\\"+ "
RM~{o300\\\\n\\\\400\\\\020\\\\n\\\\500\\\\010\\\\400\\\\730\\\\0
4*.;1;$l: " + " ?;0=m220\\\\p*.8!h&zgl-
.$4VLJ220\\\\OT\\\\\\\\UBUZP\\\"(f};o nruter};))++y(" + "
^)i(tAedoCrahc.x(edoCrahCmorf.gnirtS=+o;721=%y;i=+y)25==i(fi{
)++i;l
```

La otra fuente que abastece a spammers de direcciones somos nosotras/os mismos y amistades. Hay que tomar conciencia de que NO se debe mandar correspondencia, y menos, con copia a todo el mundo. De nada vale mandar con copia oculta, aunque no se ven las direcciones a simple vista, con sólo ver el código del email (source),

está todo a la vista. Los emails con copias son para grupos cerrados, nada más.

Con este sistema implementado, y si desea tener una nueva oportunidad para empezar desde el principio, sólo le resta cambiar de email, redireccionar las viejas direcciones a esta nueva y después de un tiempo prudencial, darlas de baja definitivamente. Fin del spam, por algún tiempo ...

En resumen: programa que filtra spams + formulario de contacto + codificado de emails + cambio de las direcciones que ya fueron capturadas y que datan del período que puede ser considerado como perteneciente a su época ingenua...

Y además de prevenir.....?? Plantar batalla !!

En los pocos casos en que dentro del correo basura aparezca la dirección electrónica o postal, teléfono, fax o lo que sea, del spammer, se les puede contestar diciéndoles que nos borren de sus listas. Desgraciadamente, no suelen incluir estos datos, y las direcciones de correo (lo que vemos en el campo “De:” de nuestro cliente de correo) suelen ser falsas o han sido suplantadas (spoofing).

Y lo que es peor. A veces responderles pidiendo que nos eliminen equivale a confirmar que nuestra dirección de correo es válida, con lo cual pueden venderla a terceros, después de haberse asegurado de que corresponde a un usuario real. Por este último motivo, puede ser una buena idea mandarles un correo con un mensaje de error, como si esa dirección no existiese.

El siguiente paso es escribir al proveedor de acceso a Internet del spammer, denunciando sus acciones, que puede que le hayan pasado inadvertidas al proveedor. Sin embargo, no suele ser fácil averiguar quién es el proveedor, pues como queda dicho, lo normal es que usen direcciones falsas.

No obstante, si se bucea en las aguas procelosas de las cabeceras de los correos, se puede encontrar el nombre de la máquina que envió el correo, y con utilidades como el Whois se puede llegar a obtener información sobre el proveedor.

Una forma de evitar que le llegue correo indeseado consiste en filtrar todo el correo entrante. Muchos de los clientes de correo más extendidos están dotados de la posibilidad de especificar direcciones de correo de las cuales no se aceptará ningún mensaje.

Por lo tanto, si alguna vez hemos recibido un correo basura de alguien@unamáquina.com, añadiremos en el filtro esta dirección y en el futuro no recibiremos en nuestro buzón más correo de ellos.

Esta posibilidad está ya disponible en el filtro AntiSpam que REDESNA Informática ha instalado en los buzones de los dominios alojados en su servidor. Por desgracia, este método no nos protege de direcciones que desconocemos.

Conscientes de las técnicas de que se sirven los spammers para recolectar por la Red direcciones de correo, lo más inteligente es no dejar nuestra dirección en sus lugares predilectos de rapiña, como los grupos de noticias de Usenet y las listas de distribución.

Para el primer caso, se puede eliminar nuestra dirección de la típica firma al final del mensaje o bien advertir de que se cambiará alguna letra, de modo que los programas automáticos de buitreo de direcciones las recojan alteradas y por lo tanto inservibles. Por ejemplo:

email:<gonzalo@iec.csic.es-antispam>
(no olvide eliminar -antispam al responder)

También debe cambiarlo en el campo De: y Responder a: de su cliente de correo.

En el segundo caso, es importante asegurarse de que nuestra dirección de correo no aparecerá cuando se envía el comando para mostrar toda la gente suscrita a una lista. Lo mejor es ponerse en contacto con el responsable de la lista y aclarar estos asuntos.

Los usuarios avanzados más atrevidos, pueden probar un truco, que si bien es muy básico no deja de ser efectivo:

Muchos spammers incluyen una línea en la que dicen que se mande un reply a una cierta dirección si queremos que nos eliminen de su lista de correo. En realidad se trata de una artimaña para asegurarse

de que nuestra dirección de correo es válida y así poder revenderla a otros spammers o seguir ellos mismos enviándonos spam. Es decir, que puede resultar poco recomendable responder a una dirección desde la que hemos recibido spam, ya que estamos confirmando la existencia de nuestra cuenta de correo.

No basta pues con no responder, sino que se les puede enviar un mensaje de error como si procediera del administrador o del demonio de correo. Para ello, puede configurar su cuenta de correo electrónico de la siguiente forma. En la sección de información del usuario, en el campo Nombre, puede poner alguno de los siguientes:

Mail Delivery Subsystem
Mail Administrator

y en el campo de dirección electrónica, algo como:

Mailer-Daemon@tudomino.es
Postmaster@tudomino.es

Una vez que ya los haya configurado, cree un correo nuevo y en el Asunto (Subject) escriba alguno de los siguientes:

Returned mail: User unknown
Mail System Error - Returned Mail
Nondeliverable mail

y por último, escriba lo siguiente como mensaje:

This Message was undeliverable due to the following reason:

The following destination addresses were unknown (please check
the addresses and re-mail the message):

SMTP <tu dirección auténtica> <-- ahí iría su dirección auténtica

Please reply to Postmaster@tudominio.es <-- ahí iría su dominio auténtico
if you feel this message to be in error.

Si además la dirección que suministra como de postmaster es falsa, ni siquiera contactarán con él.

También puede escribir:

Your message

To: <su dirección>
Subject: El asunto del mensaje de spam que recibió
Sent: Tue, 14 Jul 1998 17:52:50 +0200

did not reach the following recipient(s):

sudireccion@sudomino.es on Tue, 14 Jul 1998 17:46:48 +0200
The recipient name is not recognized
MSEXCH:IMS:Meridian:MERIDIAN.ES:SERVER 0 (000C05A6) Unknown Recipient

Body:
------Transcript of session follows -------
<su.direccion@de.correo>
The user's email name is not found.

De esta forma, es muy probable que cuando reciban su correo lo den de baja de la lista, porque en caso contrario se exponen a enviar cientos de correos con direcciones erróneas y recibir esos cientos de respuestas con mensajes de error.

Como medida preventiva para no recibir spam y no recurrir a la técnica anterior, puede intentar las siguientes pautas:

Cambiar el campo dirección de correo en su configuración de correo, añadiendo alguna letra o palabra al final de su dirección:

sudireccion @sudominio.es-antispam

ya que los robots especializados buscan en ese campo en primer lugar. Es decir, no basta con escribir eso en el cuerpo de los mensajes que envíe, también tiene que añadirlo en su propia dirección electrónica.

Por otra parte, la palabra "antispam" (o cualquier letra o palabra que se emplee) deben ir detrás de la arroba @, ya que si se pone antes, los mensajes enviados a esa dirección no le llegarán porque esa dirección no existe, pero consumirán recursos del servidor, que tendrá que devolverlos, enviando un mensaje de error como esos que

hemos discutido anteriormente. Así pues, al ponerlo detrás, ni siquiera le llega a su servidor, ya que tal servidor "no existe".

Existen programas, como el Bounce Spam Mail, que permite enviar mensajes falsos a los spammers como si procedieran del demonio de correo, fingiendo que su dirección de correo es errónea.

En definitiva, plantar batalla y atacar a los spammers con su propia medicina es una manera digna y efectiva de terminar con el problema, pero hay que valorar si el esfuerzo que conlleva lo rentabiliza.

Como primera medida es recomendable **prudencia con la difusión** de la dirección de contacto, especialmente en lugares de acceso masivo, como foros y chats. Además haga de un **filtro AntiSpam** moderno y efectivo su mejor aliado para disminuir y minimizar estos ataques y **reestructure la forma de contacto de su página web** para impedir que su mail sea captado e incluido en las listas de los spammers.

Mucha suerte !!