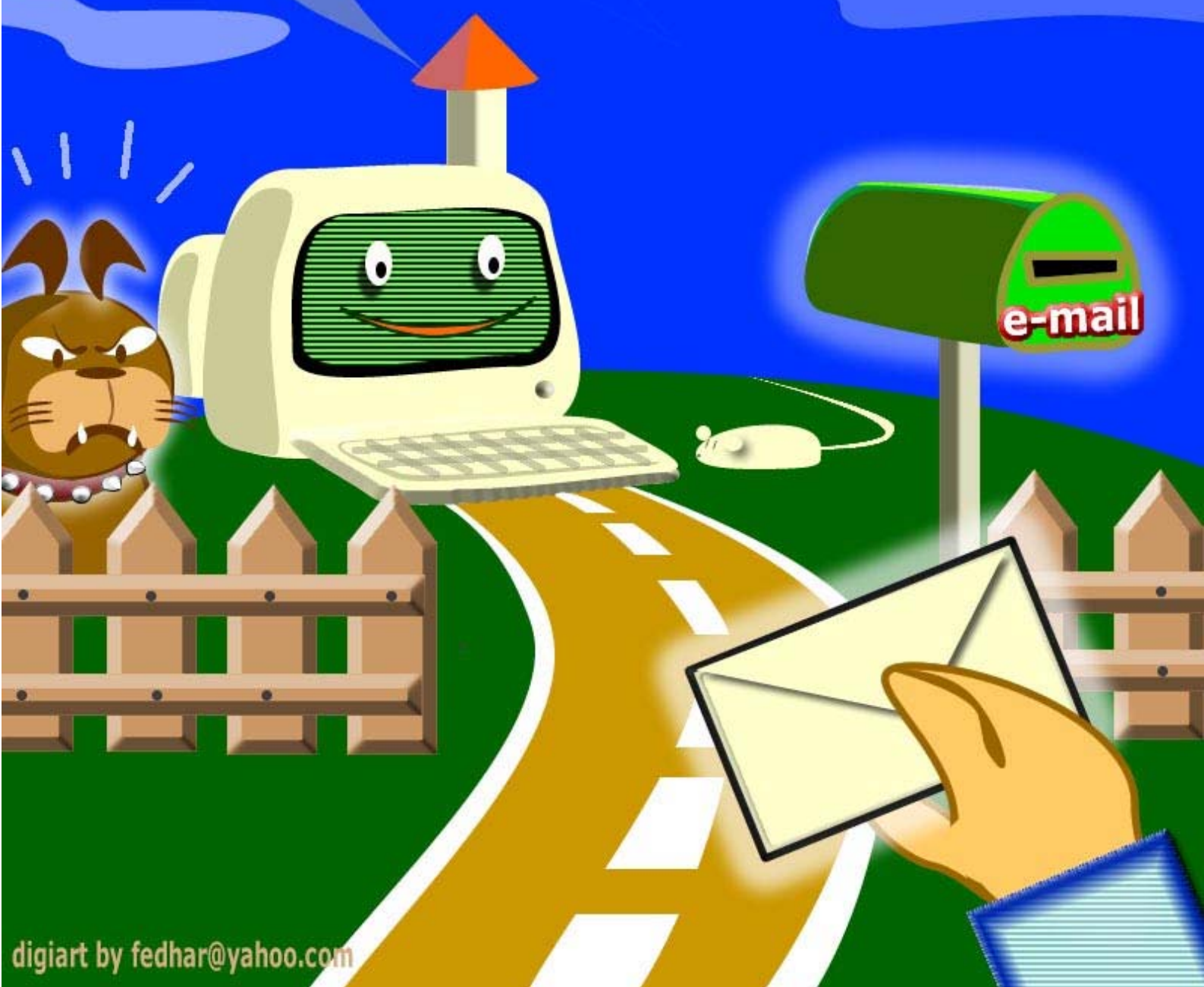


Eugenio Siccardi

Guía de uso del correo electrónico

Pautas de comportamiento
para una comunicación electrónica
grata y productiva



Eugenio Siccardi

Guía de uso del

correo electrónico

**Pautas de comportamiento
para una comunicación electrónica
grata y productiva**

Para contactar al autor

info@rompecadenas.com.ar

<http://www.rompecadenas.com.ar>

Este libro puede descargarse en forma gratuita de

<http://www.rompecadenas.com.ar/guiacorreio.htm>

Diseño y diagramación

Yanina Siccardi

Ilustración de tapa y digiart

by Fedhar

fedhar@yahoo.com

(c) 2002 - Eugenio Siccardi

1ª edición - Julio 2002

ISBN 987-43-4880-1

Las marcas mencionadas en este libro son marcas registradas de sus respectivos titulares.

Índice

6 ▶ **Presentación**

7 ▶ **Introducción**

Cómo usar el correo electrónico

9 ▶ **Netiquette** (la etiqueta de la red)
Algunas reglas para el buen comportamiento en Internet.

12 ▶ **Reenviar mensaje**
Seguramente sabés cómo hacer esto. Pero no te lo saltees. Esta opción es en gran medida la culpable de la falta de privacidad de las direcciones de mail.

14 ▶ **Responder al autor**
Cómo responder correctamente un mensaje.

15 ▶ **Responder a todos**

16 ▶ **Enviar mensaje a un grupo**
Cómo enviar un mensaje a un grupo de destinatarios sin revelar sus direcciones.

17 ▶ **Envío de archivos adjuntos**
No te voy a enseñar cómo adjuntar un archivo sino por qué NO adjuntarlo.

20 ▶ **Mensajes en formato HTML**
Bonitos pero conflictivos.

22 ▶ **Configuración de nuestra cuenta de correo**
Si no queremos perder ningún mensaje es imprescindible configurar correctamente nuestra cuenta de correo electrónico.

26 ▶ **Firma automática**

- 27** ▶ **Backup**
Algo de lo que siempre nos acordamos cuando ya es tarde: hacer un backup de nuestra libreta de direcciones y de los mensajes importantes.
- 29** ▶ **¿Por qué no llegan los mails que mando?**
Esos malditos mensajes de rechazo que siempre están en inglés!

Cómo NO usar el correo electrónico: abusos cometidos con el mail

- 33** ▶ **Hoaxes**
Cadenas de solidaridad para ayudar a niños enfermos, alertas sobre virus que no existen, métodos infalibles para hacerse millonario. Sólo un pequeño porcentaje de estos mensajes que inundan nuestro buzón es cierto.
- 45** ▶ **Spam**
Quienes tenemos una cuenta de correo electrónico recibimos habitualmente mensajes publicitarios no solicitados, una práctica que perjudica a todos.
- 53** ▶ **Virus**

Información complementaria

- 57** ▶ **Enlaces**
- 60** ▶ **Distribución de este e-book**
- 61** ▶ **Acerca del autor**
- 62** ▶ **Acerca de Rompecadenas**
- 63** ▶ **Colaborar con Rompecadenas**
- 65** ▶ **Agradecimientos**

Presentación

El correo electrónico acerca a las personas, ayuda a encontrar familiares y amigos alrededor del mundo, es más barato que el teléfono o el correo postal, es una excelente herramienta comercial.

Pero también puede causarnos muchos problemas:

- ▶ podemos vernos bombardeados por publicidad no solicitada (spam);
- ▶ vernos engañados con falsas cadenas de solidaridad o métodos para hacernos millonarios (hoaxes);
- ▶ recibir virus que afecten nuestra computadora.

Además, pueden sucedernos muchas otras cosas: que nos envíen archivos muy grandes y no podamos descargarlos, que recibamos o enviemos mensajes que no se entiendan, que perdamos nuestra libreta de direcciones, y muchos otros detalles que pueden hacer que una herramienta tan eficaz como el correo electrónico se convierta en una molestia.

¿Para qué puede servirte este libro? Para no tener problemas con tus mails, para que los destinatarios de tus mensajes puedan comprender claramente lo que querés transmitirles, para proteger tu cuenta de correo (y tu privacidad) en todo lo que dependa de vos, para proteger la información almacenada en tu computadora.

Para utilizar el mail es necesario, además de saber manejar el programa, aprender algunas otras cosas.

En este libro encontrarás algunas pautas que ayudarán a que tu comunicación electrónica sea una experiencia grata y productiva.



▶ **Para utilizar el mail es necesario, además de saber manejar el programa, aprender algunas otras cosas.**

▶ **En este libro encontrarás algunas pautas que ayudarán a que tu comunicación electrónica sea una experiencia grata y productiva.**

Introducción

Este libro contiene algunos principios que te ayudarán a utilizar eficazmente el correo electrónico.

No es un manual de uso de ningún programa de correo, aunque a veces nos referiremos a alguno en particular.*

Es más bien una guía de comportamiento para la comunicación electrónica.

Está dirigido a aquellas personas que ya poseen los conocimientos básicos sobre la utilización de su programa de correo electrónico, es decir, saben cómo enviar y recibir mails, qué es un archivo adjunto, etc., pero se encuentran con algunos problemas en el manejo cotidiano de su correspondencia electrónica.

Algunas de las reglas aquí mencionadas pueden ser aplicadas a los distintos servicios de Internet (chat, listas de discusión, etc.) pero nos centraremos especialmente en el correo electrónico por ser el más difundido.

El libro se compone básicamente de 2 secciones:

Cómo usar el correo electrónico.

Nos referiremos aquí a todas las cuestiones que hacen que un mensaje de correo electrónico pueda llegar a destino y sea leído y comprendido por el destinatario sin ningún problema.

Cómo NO usar el correo electrónico: abusos cometidos con el mail.

En esta sección nos centraremos en las malas prácticas en que incurren los usuarios de correo electrónico, ya sea por desconocimiento o mala intención (hoaxes, spam, envío de virus) y cómo protegerse de ellas.

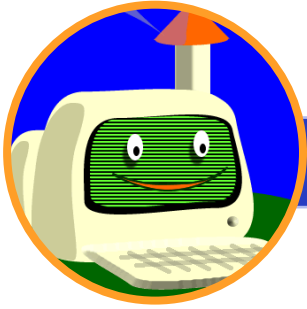
Espero que este libro te sea de utilidad.

Eugenio Siccardi

El Bolsón, Patagonia, Argentina

Julio 2002

* Para los ejemplos utilizaremos Outlook Express.



Cómo usar

el correo electrónico



Netiquette

El término *Netiquette* (la etiqueta de la Red) designa a un conjunto de reglas para el buen comportamiento en Internet.

Estas reglas no son caprichosas sino que están respaldadas por la experiencia de quienes hace años utilizan el correo electrónico y son la base en la que se apoya una comunicación electrónica fluida y efectiva.

Hay reglas específicas para los distintos servicios de Internet (listas de discusión, chat, foros, FTP, etc.).

Las que siguen son algunas de las que pueden aplicarse al correo electrónico:

1. Identificación clara del remitente y el destinatario

En una casa u oficina, puede ocurrir que varias personas utilicen la misma computadora y la misma cuenta de mail.

Por lo tanto:

- ▶ Debemos escribir el nombre de la persona a la que va dirigido el mail.
- ▶ También debemos firmarlo.

No es agradable recibir un mail que diga solamente "*el envío fue despachado ayer*".

Recibo en mi trabajo varios mails de este tipo a la semana. Como no tienen ni remitente ni destinatario, van a parar a la basura ya que no sé de quién vienen ni a quién debo entregarlo.

2. Privacidad

El mail no es tan privado como parece.

Debemos tener cuidado con lo que escribimos. Otras personas pueden leerlo, ya sea en nuestra computadora, en la del destinatario o porque éste lo reenvía.

3. Del otro lado hay seres humanos

No olvidar que, aunque estemos mirando un monitor, lo que escribimos lo leerá una persona. Si recibimos un mail que nos disgusta, lo mejor es esperar al día siguiente para contestarlo y no escribir algo de lo que después nos arrepintamos.



- ▶ **Escribir el nombre de la persona a la que va dirigido el mail.**
- ▶ **El mail no es tan privado como parece.**
- ▶ **Aunque estemos mirando un monitor, lo que escribimos lo leerá una persona.**

4. Cadenas

No reenviar ninguna cadena de mails. La inmensa mayoría son falsas y algunas pueden ser muy perjudiciales.

5. Alertas de virus

No reenviar ningún alerta de virus. La mayoría son falsos. Podés mantenerte actualizado sobre nuevos virus suscribiéndote a los boletines de los sitios especializados. Encontrarás algunas direcciones en la página de enlaces y en el *Directorio Rompecadenas*.

6. Mensajes publicitarios no solicitados (spam)

No enviar nunca mensajes publicitarios no solicitados.

Si querés promocionar tu negocio o tu página web, conseguí las direcciones de forma lícita, por ejemplo, poniendo un formulario en tu página o creando un boletín.

Jamás compres o vendas direcciones de mail.

7. No responder ningún mensaje no solicitado

No responder ningún mensaje no solicitado ni siquiera con la palabra *REMOVE* o *UNSUSCRIBE* ya que respondiendo estamos diciendo que nuestra dirección es válida.

Los spammers utilizan esta técnica para confirmar las direcciones con lo cual, en vez de dejar de recibir mensajes, comenzamos a recibir más.

8. Subject o Asunto

No envíes un mensaje sin *Subject*.

En el *Subject* o *Asunto*, describí breve y claramente el contenido del mail.

9. ¿De qué estás hablando?

No respondas un mail diciendo solamente "OK" o "Yo no".

Explicá en forma concisa de qué estás hablando.

10. No incluir todo el mensaje original en la respuesta

No incluyas, en la respuesta a un mensaje, todo el mail original.

Suprimí lo que no sirva, dejando solamente lo necesario para darle contexto a tu respuesta.

11. Reenviar mensajes

Si recibís un mail y querés reenviarlo asegurate de borrar todas las direcciones que aparecen en el mensaje.



- ▶ No reenviar cadenas de mails.
- ▶ No reenviar alertas de virus.
- ▶ No enviar publicidad no solicitada.
- ▶ No enviar mensajes sin *Asunto*.
Describí breve y claramente el contenido.
- ▶ No incluir todo el mail original en la respuesta.
- ▶ Al reenviar un mail, borrar todas las direcciones que aparecen en el cuerpo del mensaje.

12. Enviar un mensaje a un grupo

Utilizá el campo "CCO" o "BCC" para escribir las direcciones cuando quieras enviar un mail a varias personas.

De esta manera evitás que todos conozcan las direcciones del resto de la lista.



- ▶ Utilizar el campo "CCO" o "BCC" al enviar un mensaje a varias personas.
- ▶ No escribir todo el mensaje en mayúsculas.

13. No utilizar MAYUSCULAS

NO ESCRIBAS TODO EL MENSAJE EN MAYUSCULAS. Es cansador para leer e implica estar GRITANDO.

¿Cansado de que tus amigos
te pidan Solidaridad con Brian?

Atrevete a romper las cadenas

<http://www.rompecadenas.com.ar>



Reenviar mensaje

Esta sencilla opción, mal utilizada, es una de las principales causantes de la falta de privacidad en Internet.

Todos los programas de correo electrónico disponen de ella y es muy útil cuando queremos reenviar a otra persona un mensaje que recibimos ya que:

- ▶ Incorpora al nuevo mensaje el mensaje original.
- ▶ Incorpora al nuevo mensaje el subject o asunto original.
- ▶ Sólo debemos introducir la dirección del destinatario en el campo correspondiente.

El problema radica en lo siguiente: incorpora al nuevo mensaje la dirección del remitente original.

De esta manera, cuando un mensaje se transforma en cadena, todas las direcciones anteriores van siendo incorporadas a los nuevos mensajes y vistas por todos los que lo reciben.

Si alguno de los que lo reenvían, lo manda a toda su libreta de direcciones, todas estas direcciones se agregarán a los sucesivos reenvíos.

Así es como recibimos mails con cientos de direcciones en el cuerpo del mensaje pero el texto del mensaje ocupa 5 líneas. Y ésta es también una de las formas en que las personas que venden direcciones de mail a los spammers arman sus bases de datos.

Soluciones

- ▶ **No reenviar cadenas de mensajes.**

La mayoría de los mensajes que vienen en cadena no merecen la pena de ser reenviados ya que casi todos son falsos o engañosos (ver *Hoaxes*).

Al reenviar un mensaje, utilizando la opción *Reenviar mensaje* o *Forward* del programa de correo, se incorporan al nuevo mensaje todas las direcciones incluidas en los campos *Para* y *CC*.



▶ **Esta opción, mal utilizada, es una de las principales causantes de la falta de privacidad en Internet.**

▶ **No reenviar cadenas de mensajes.**

Para evitar esto, si deseás reenviar a varias personas un mensaje que recibiste, procedé de la siguiente manera:

- ▶ Seleccioná la parte del mensaje que deseás reenviar, evitando las direcciones.
- ▶ Copiá y pegá en un mensaje nuevo.
- ▶ También podés clicar en *Reenviar* y eliminar las direcciones del cuerpo del mensaje.

De esta manera evitás que circulen todas las direcciones que venían en el mail.

Siguiendo estos simples consejos haremos nuestro aporte para mantener la privacidad de todos en *Internet*.

Brian no existe!!!!!!!!!!!!!!!!!!!!

Mejor Rompecadenas

<http://www.rompecadenas.com.ar>

Responder al autor

Cuando alguien nos reenvía un mail de otra persona y queremos responderle al autor original, no podemos usar la opción *Responder al autor*, ya que de esta manera estaríamos respondiéndole a quien nos reenvió el mail y no a la persona correcta.

Veamos un ejemplo:

Un cliente envía un mensaje a la dirección de mail principal de una empresa (**info@empresa.com**).

Quien lo recibe, lo reenvía al departamento correspondiente a la consulta (**ventas@empresa.com**).

Si quien contesta el mensaje, lo hace utilizando la opción *Responder al autor*, la respuesta le llegará a **info@empresa.com** y no al cliente, que sería el verdadero destinatario del mensaje.

En este caso correspondería escribir el mail en un mensaje nuevo colocando en el campo *Para* la dirección del cliente.

Es muy habitual que se produzcan estas confusiones que, en ocasiones, pueden llegar a causar verdaderos problemas.

He sido testigo de algunas situaciones desagradables por esta causa.

Por ejemplo, **A** recibió de **B** algo que envió **C** y en lugar de escribirle a **C** en un mensaje nuevo hizo click en *Responder al autor*.

Le agregó algunos comentarios criticando a **B** y lo envió.

El mensaje lo recibió **B** y no **C**.

No sé qué habrá pasado luego entre ellos, pero este tipo de situaciones puede ser causa de disgustos, peleas, etc.

Por lo tanto, no es mala idea antes de enviar el mail, chequear si la dirección a la que queremos que llegue es la correcta.



▶ Cuando alguien nos reenvía un mail de otra persona y queremos responderle al autor original, no podemos usar la opción *Responder al autor*.

▶ Escribir el mail en un mensaje nuevo, colocando en el campo *Para* la dirección del autor original.

▶ Antes de enviar el mail, chequear si la dirección a la que queremos que llegue es la correcta.

Responder a todos

La opción *Responder a todos* no es muy utilizada. Podemos usarla básicamente cuando estamos intercambiando información con un grupo de personas.

Pero además de los puntos tratados en el capítulo *Netiquette* sobre cómo responder un mensaje, conviene tener en cuenta lo siguiente:

- ▶ cuando recibimos un mensaje que fue enviado también a otras personas y utilizamos la opción *Responder a todos*, el mensaje que redactemos será enviado a todas las direcciones que venían en los campos *Para* y *CC*.

Esta es una opción que hay que utilizar con mucho cuidado ya que puede sucedernos creer estar respondiéndole sólo al autor y en realidad nuestra respuesta es recibida por varias personas a las que no les interesa o que no queremos que la lean.



▶ **Cuando recibimos un mensaje que fue enviado también a otras personas y utilizamos la opción *Responder a todos*, el mensaje que redactemos será enviado a todas las direcciones que venían en los campos *Para* y *CC*.**

Enviar mensaje a un grupo



- ▶ **Enviar un mensaje a un grupo de destinatarios puede ser el causante de la pérdida de privacidad de sus direcciones.**
- ▶ **Utilizar el campo "CCO" o "BCC".**
- ▶ **A veces, al enviar una nota de prensa por ejemplo, conviene enviar los mails uno por uno, en lugar de realizar un envío masivo e impersonal.**

Como vimos en la *Netiquette*, enviar un mensaje a un grupo de destinatarios puede ser la causa de la pérdida de privacidad de sus direcciones.

Para enviar un mensaje a un grupo sin revelar sus direcciones, hay que proceder de la siguiente manera:

- ▶ **Utilizá el campo "CCO" o "BCC".**

Todas las direcciones que incluyas en estos campos no serán vistas por las personas que reciben el mensaje. Lo que verán los destinatarios será, por ejemplo, la leyenda *Undisclosed Recipients*.

Dependiendo del tipo de mensaje que estamos enviando, o si se trata de un grupo de personas con las que no tenemos un trato habitual, tal vez convenga hacer un envío personalizado en lugar de uno masivo e impersonal.

Si estamos enviando, por ejemplo, una gacetilla o una nota de prensa, es mucho mejor enviar uno por uno los mails agregando el nombre, en este caso, del redactor o periodista a quien va dirigido.

Esto generará mayor respuesta a tu mensaje ya que se trata de una comunicación personal y no grupal.

Por otro lado, en ocasiones es conveniente y hasta "ético", por decirlo de alguna manera, que se vean las direcciones de las personas a quienes estamos enviando el mail.

Por ejemplo, si estamos estableciendo una comunicación con varias personas que se conocen (me refiero a una comunicación verdadera, no a reenviar una cadena), es de muy mal gusto ocultar las direcciones, ya que de esta forma el receptor no sabe que otros también están recibiendo el mensaje.

Envío de archivos adjuntos



Por el momento y debido al pobre ancho de banda con que aún cuenta la gran mayoría de los usuarios, debe tenerse mucho cuidado con el envío de archivos adjuntos ya que demoran más tiempo en descargarse y, por otro lado, pueden contener virus.

Un archivo de 1 Mb puede tardar en descargarse hasta 15 minutos o más, dependiendo del tráfico del servidor de destino y la velocidad del modem del destinatario.

No nos molestaría recibir un archivo de 1 Mb importante para nuestro trabajo pero si estamos 15 minutos bajando un archivo y después resulta que se trata de una bonita tarjeta animada podemos llegar a molestarnos con la persona que la envió.

La primera que recibimos puede resultarnos divertida. A la décima, comenzaremos a maldecir. A la Nº 100 querremos romper todo.

Un fin de año recibí una tarjeta que pesaba 2 Mb y quiero utilizar este ejemplo para mostrar cómo una simple tarjeta de fin de año puede afectar el rendimiento de toda la red.

La tarjeta, como dije, pesaba 2 Mb y fue enviada a unas 50 personas (dicho sea de paso, la persona que la envió escribió las direcciones en el campo CC en lugar del campo CCO, con lo cual los 50 nos enteramos de las direcciones de todos).

El envío de esta tarjeta insumió:

- ▶ 50 mails x 2 Mb = 100 Mb de espacio en el disco del servidor de origen (y muchos otros recursos, ya que la mayoría de los programas de correo electrónico envían un solo mail. El servidor se encarga de preparar los 50 mails iguales, uno con cada dirección).
- ▶ 50 mails x 2 Mb = 100 Mb de espacio en los distintos servidores de destino.
- ▶ Total: 200 Mb (sin contar con las devoluciones por direcciones inexistentes o por servidores con límites en el tamaño de los archivos).



- ▶ **Tener mucho cuidado con el envío de archivos adjuntos ya que demoran más tiempo en descargarse y pueden contener virus.**
- ▶ **La primera tarjeta animada de varios Mb que recibimos puede resultarnos divertida. A la décima, comenzaremos a maldecir. A la Nº 100 querremos romper todo. Sobre todo si contamos con una conexión dial up.**



- ▶ **Que el archivo sea importante para el destinatario.**
- ▶ **Recordar que el envío y la descarga de mails insumen tiempo y dinero.**
- ▶ **No enviar archivos de gran tamaño.**
- ▶ **Asegurarnos de que el destinatario puede recibirlos.**
- ▶ **No todos disponen de conexiones de banda ancha.**
- ▶ **Asegurarnos de que el archivo salga sin virus.**

Una sola tarjeta ocupó 200 Mb durante un tiempo (este tiempo será variable, pero puede llegar a ser de varios días).

Es incalculable la cantidad de tarjetas que se envían en las fiestas de fin de año, pero supongo que serán unos cuantos millones. Los números son escalofriantes.

Por eso, es conveniente restringir el envío de archivos adjuntos.

En conclusión, debemos tener en cuenta los siguientes puntos:

- ▶ Que el archivo sea importante para el destinatario.
- ▶ Recordar que el envío y la descarga de mails insumen tiempo y dinero.
- ▶ No enviar archivos de gran tamaño (he visto gente intentar enviar archivos de 28 Mb a través de una conexión dial-up a 33600 bps).
- ▶ Si tenemos necesidad de enviar archivos de gran tamaño (mayores de 1 Mb) debemos asegurarnos de que el destinatario puede recibirlos:
 - ▶ Hay servidores, sobre todo los que ofrecen direcciones de mail gratuitas, que no aceptan archivos de gran tamaño (en general, el límite es 1 Mb).
 - ▶ Estos mismos servidores tienen un límite en la cantidad de información que puede almacenar la cuenta de mail. Si la casilla está llena, nuestro mail no entrará.
 - ▶ Hay usuarios que disponen de conexiones lentas con lo cual un mail de gran tamaño tardará mucho en bajar o incluso no podrá hacerlo y trabará la descarga de sus mails. Recordar que no todos disponen de conexiones de banda ancha. Con el advenimiento de la banda ancha, los usuarios que disponen de ella, comenzaron a enviar indiscriminadamente archivos descomunales. Si quien los recibe también dispone de una conexión de este tipo no tendrá problemas. Pero si se conecta a través de la línea telefónica no le agradará que le envíen un video de 20 Mb que no le interesa y le impide descargar su correo con normalidad.
- ▶ No enviar el archivo adjunto solamente, sino saludar, firmar y colocar una leyenda en el cuerpo del mensaje diciendo algo así como *"adjunto te envío información sobre tal tema"* para que el desti-



- ▶ **No escribir un mensaje en un procesador de texto y enviarlo como adjunto.**
- ▶ **No obligues al destinatario a tener que abrir otro programa innecesariamente.**
- ▶ **No todos utilizan el mismo procesador de texto.**

natario esté seguro de que no se trata de un virus enviado en forma automática desde una computadora infectada. Lo mejor es poner además el nombre del archivo.

- ▶ Asegurarnos de que el archivo salga sin virus.
- ▶ No escribas un mensaje en un procesador de texto y lo envíes como adjunto, cuando podés escribirlo directamente en el cuerpo del mensaje.

No obligues al destinatario a tener que abrir otro programa innecesariamente para leerlo.

No todos utilizan el mismo procesador de texto y tal vez algunos no puedan abrir el archivo.

Además, aumentás las posibilidades de enviar un virus y tu mensaje será mucho más "pesado" y tardará más en bajar.

Como ejemplo, el párrafo anterior escrito directamente en el mensaje, en sólo texto, "pesa" 2 kb, mientras que en un archivo de Word "pesa" 19 kb.

Casi 10 veces más.

¿Microsoft y AOL pagarán u\$s 245 por cada email reenviado?

ja ja ja!

Atrevete a romper las cadenas

<http://www.rompecadenas.com.ar>

Mensajes en formato HTML



- ▶ **Los mensajes en formato HTML están expuestos a muchas vulnerabilidades.**
- ▶ **Ocupan un tamaño mucho mayor que el mismo mensaje en sólo texto.**
- ▶ **Hay personas que utilizan programas que no pueden leer este formato.**

No recomiendo la utilización de mensajes en formato HTML por las siguientes razones:

- ▶ Están expuestos a muchas vulnerabilidades que permiten la potencial ejecución de código maligno. Por ejemplo, la mayoría de los virus más difundidos últimamente (como el *Klez* o el *Badtrans*) utilizan el formato HTML de los mensajes de correo electrónico.
- ▶ Un mensaje en formato HTML ocupa un tamaño mucho mayor que el mismo mensaje en sólo texto.
- ▶ Hay personas que utilizan programas que no pueden leer este formato, con lo cual tu mensaje se verá lleno de caracteres extraños.
- ▶ Por otro lado, sucede una cosa bastante molesta con los programas que sí pueden leerlo. Si utilizás una conexión dial-up y tenés configurado tu programa de correo para que cuelgue la conexión telefónica una vez que terminó de recibir los mensajes, puede suceder que los mensajes en formato HTML no hayan terminado de bajar completamente (o sea, entra el HTML pero no las imágenes incrustadas), con lo cual cada vez que selecciones este mensaje para leerlo, se disparará automáticamente la conexión de acceso telefónico para intentar descargar las imágenes.

Esta es la razón por la cual algunas personas encuentran que su computadora está conectada sin que ellos se hayan dado cuenta.

Por estas razones, creo que el envío de mensajes en formato de sólo texto aun sigue siendo la mejor opción.

Para que tus mensajes sean enviados en formato de sólo texto, es necesario ir a *Herramientas > Opciones > Enviar* y en *Configuración de formato de envío de correo* elegir la opción *Texto sin formato*.

También recomiendo desactivar la opción *Responder a los mensajes en el formato en el que se enviaron* ya que si recibís un mensaje en

HTML, al responderlo estarás enviando también un mensaje en ese formato.

Si alguna vez necesitás enviar un mensaje en HTML, podés elegir esta opción únicamente para ese mensaje.

Vas a *Crear correo* y en el nuevo mensaje elegís *Formato > Texto enriquecido (HTML)*.



Configuración de nuestra cuenta de correo



Es fundamental que nuestro programa de correo esté bien configurado con todos nuestros datos para que no se nos pierdan mensajes y para que los destinatarios sepan rápidamente quién les está escribiendo.

Todos los programas de correo tienen opciones similares, aunque para los ejemplos nos basaremos en *Outlook Express*.


Para verificar que la cuenta esté bien configurada, tenemos que ir a *Herramientas > Cuentas > Correo* y hacer doble click sobre nuestra cuenta.

En *General* veremos algo así:

Propiedades de rompecadenas [?] [X]

General | Servidores | Conexión | Seguridad | Avanzada

Cuenta de correo _____

 Escriba el nombre que prefiere para referirse a los servidores. Por ejemplo, "Trabajo" o "Servidor de correo de Microsoft".

rompecadenas

Información de usuario _____

Nombre: Rompecadenas

Organización: _____

Dirección de correo electrónico: info@rompecadenas.com.ar

Dirección de respuesta: _____

Incluir la cuenta al recibir correo electrónico o sincronizar

Nombre

Puede ser el nombre y apellido si es de una persona o el nombre o razón social si es una empresa.

Puede parecer redundante detenernos en este punto pero muchas personas en vez de su nombre o el de su empresa colocan aquí sus sobrenombres o cosas más disparatadas como el nombre de sus mascotas o el de su dibujo animado preferido, con lo cual el destinatario no tiene idea de quién le está escribiendo

Si encima el remitente no firma el mensaje, nadie sabrá quién lo escribió.

Dirección de correo electrónico

Aquí debemos colocar nuestra dirección de correo teniendo especial cuidado en que esté bien escrita.

Aunque parezca mentira, hay mucha gente que escribe mal su propia dirección de mail.

Si la escribimos mal todas las personas que reciban nuestros mails e incorporen nuestra dirección a su libreta, la tendrán equivocada y cada vez que nos escriban el mensaje se perderá.

También sucederá lo mismo cuando alguien responda a nuestros mensajes utilizando la opción *Responder al autor*.



► **Colocar nuestra dirección de correo teniendo especial cuidado en que esté bien escrita.**

Dirección de respuesta

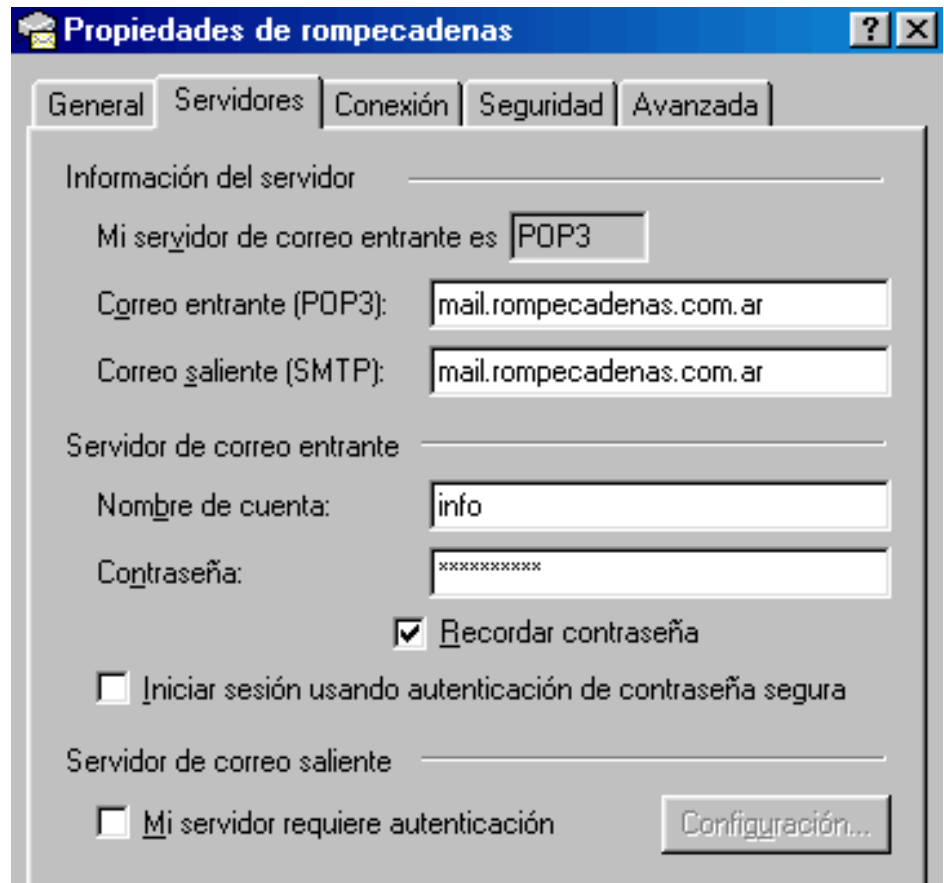
Si no colocamos nada aquí, la dirección de respuesta por defecto será la misma que hayamos ingresado en *Dirección de correo electrónico*.

Incluir la cuenta al recibir correo electrónico o sincronizar

Si esta opción está activada se descargarán los mensajes entrantes de esta cuenta al pulsar el botón *Enviar y recibir*.

Si no está activada, no se descargarán aunque sí podremos enviar mensajes con esta dirección.

Si pulsamos en *Servidores* tendremos las siguientes opciones:



Los datos que figuran aquí son fundamentales para que podamos enviar y recibir mails.

Correo entrante / Correo saliente

Aquí deberemos escribir los nombres de nuestros servidores de correo. Si no los conocemos tendremos que preguntarlos al Administrador del servidor.

Nombre de cuenta

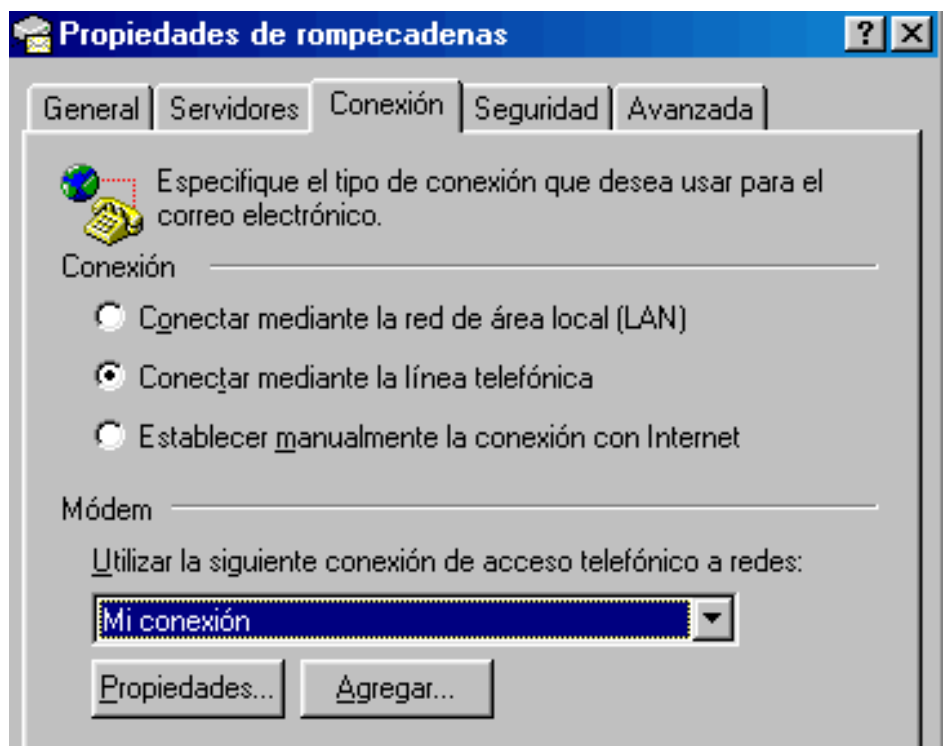
Aquí colocaremos nuestro nombre de usuario (en algunos servidores el nombre de usuario es la dirección de mail completa y en otros solamente lo que está antes de la @).

Contraseña

Si la escribimos aquí y además activamos la opción *Recordar contraseña*, no tendremos que ingresarla cada vez que queramos conectarnos.

Finalmente, tendremos que vincular nuestra cuenta de correo con la conexión de *Acceso telefónico a redes*.

Para ello vamos a *Conexión*:



Elegimos *Conectar mediante la línea telefónica* (si utilizamos una conexión dial-up) y, más abajo, la conexión correspondiente.

Firma automática

Una buena idea para que nuestros mensajes salgan siempre con nuestro nombre es configurar una firma automática¹.

Para hacerlo, vamos a *Herramientas > Opciones > Firmas*

Presionamos el botón *Nueva*.
Se crea la *Firma N°1*.

Podemos elegir si queremos definir allí mismo el texto que queremos utilizar como firma o podemos utilizar algún archivo de texto ya existente en nuestra PC.

Si tildamos *Texto* podemos escribir en el campo correspondiente lo que queremos que aparezca al final de nuestros mensajes.

Estos datos pueden ser nombre, apellido, url de nuestro sitio web, direcciones de mail, dirección postal, teléfono, nombre de la empresa, cargo, etc.

Pero no es conveniente extenderse demasiado: con cuatro o cinco líneas es más que suficiente.


Luego tildamos *Agregar firmas a todos los mensajes salientes*.

Si elegimos poner nuestra firma desde un archivo:

Tildamos *Archivo*, vamos a *Examinar*, y elegimos el archivo de texto que queremos que sea nuestra firma.

Si tenemos varias cuentas de correo, podemos configurar varias firmas y elegir cuál queremos utilizar en cada una.

Seleccionamos cada firma, vamos a *Opciones avanzadas* y allí elegimos la cuenta correspondiente.



X
Una buena idea para que todos nuestros mensajes salgan siempre con nuestro nombre es configurar una firma automática.

(1) Ver "Firma automática" en mi libro *Cómo escribir un mail*.



Backup



► Como con el resto de los archivos es conveniente hacer una copia de resguardo en otro sistema de almacenamiento (diskette, zip, CD) aparte del disco rígido.

Algo de lo que siempre nos acordamos cuando ya es tarde: hacer un backup de la libreta de direcciones y los mensajes.

Libreta de direcciones

Para hacer un backup de la libreta de direcciones tendremos que ir a *Archivo > Exportar > Libreta de direcciones*.

Elegimos la opción *Archivo de texto* (valores separados por comas). Aceptamos.

Luego tenemos que nombrar el archivo y elegir en qué directorio queremos guardarlo.

Se generará un archivo .csv.

Para recuperar las direcciones, si tuvimos que reinstalar Windows o Outlook Express, tenemos que ir a *Archivo > Importar > Libreta de direcciones* y buscar el archivo que generamos.

También podremos importarla a un procesador de texto o a una base de datos.

Como con el resto de los archivos es conveniente hacer una copia en otro sistema de almacenamiento (diskette, zip, CD) aparte del disco rígido.

Mensajes

Hay varias maneras de resguardar nuestros mensajes de correo electrónico.

Cada uno podrá hacerlo de acuerdo a sus gustos, necesidades, cantidad de mensajes, etc.

- Outlook Express guarda por defecto los mails en el directorio `C:\WINDOWS\Application Data\Identities\{83B7A360-3077-11D6-A1ED-FD3697536A76}\Microsoft\Outlook Express`.

El directorio `{83B7A360...}` varía de nombre en cada PC.

En ese directorio se encuentran las distintas carpetas que tenemos en Outlook Express.

Cada carpeta es un archivo que contiene todos los mails con sus archivos adjuntos.

Si queremos guardarlos en un directorio más accesible, por ejemplo *C:\Mis Documentos\Mails*, vamos a *Herramientas > Opciones > Mantenimiento > Carpeta de almacén* y allí elegimos el que queremos.

De esta forma, los mails entrarán en tu backup de datos habitual, porque periódicamente realizás un backup de tus datos ¿verdad?

- ▶ También podemos arrastrar los mails que queremos guardar a cualquier carpeta.

Tendremos que tener abiertos al mismo tiempo *Outlook Express* y el *Explorador de Windows*. Simplemente arrastramos y soltamos en la carpeta que queremos.

- ▶ Hay gente que prefiere guardar únicamente los archivos adjuntos o copiar los textos de algunos mensajes que recibió en su procesador de textos.

Para guardar los adjuntos abrimos el mail junto al cual viene, vamos a *Archivo > Guardar datos adjuntos...*, allí elegimos en cuál directorio queremos guardarlo y pulsamos *Guardar*.

Para copiar el texto de un mail lo seleccionamos, vamos a *Edición > Copiar*. Luego vamos al procesador de textos, creamos un archivo nuevo y pegamos.

- ▶ Finalmente, hay un software excelente, *Outlook Express Backup*, aunque es comercial, que nos permite guardar todas las carpetas, mails, archivos adjuntos, reglas de mensaje y favoritos de Internet en un sólo archivo.

Si tenemos que reinstalar *Outlook Express* o *Windows*, luego de hacerlo ejecutamos este archivo y volvemos a tener todo como antes.

En los *Enlaces* encontrarás una dirección para descargar una demo de 15 días.



▶ **Cambiando la carpeta de almacenamiento de los mails a una más accesible, estos entrarán en tu backup de datos habitual. Porque periódicamente realizás un backup de tus datos, ¿verdad?**

Por un correo electrónico
sin basura

Atrevete a romper las cadenas

<http://www.rompecadenas.com.ar>

¿Por qué no llegan los mails que mando?



Los mensajes de correo electrónico pueden no llegar a destino por distintas causas.

Pero la inmensa mayoría son rechazados debido a que la dirección del destinatario es incorrecta.

Hay gente que envía el mismo mensaje 10 o 15 veces hasta que llama enfurecida a la mesa de ayuda echándole la culpa al servidor de que sus mensajes no llegan.

Si recibís un mensaje de rechazo de un mail que mandaste, antes de llegar a esta situación, es conveniente leerlo para tratar de averiguar cuál es el problema.

Los mensajes de rechazo en general están escritos en inglés por lo que la mayoría de los usuarios hispanoparlantes los ignora e insiste en enviar de nuevo el mail, que, invariablemente, volverá a ser rechazado por la misma causa.

Cada servidor tiene sus propios mensajes de rechazo pero básicamente podremos encontrarnos con los siguientes casos (las direcciones son a modo de ejemplo):

▶ Servidor inexistente

Por ejemplo, el remitente escribió la siguiente dirección:

nombre_de_usuario@hotmail.com.ar

cuando la correcta hubiera sido

nombre_de_usuario@hotmail.com

El mensaje de error será:

"A mail message could not be sent because **the following host is unknown:** hotmail.com.ar"

Esto quiere decir que no se pudo encontrar el servidor de destino. Está mal escrito el nombre del servidor. No hay ningún servidor denominado *hotmail.com.ar*.



- ▶ **La inmensa mayoría de los mensajes que no llegan a destino, son rechazados debido a que la dirección del destinatario es incorrecta.**
- ▶ **Los mensajes de rechazo en general están escritos en inglés por lo que la mayoría de los usuarios hispanoparlantes los ignora e insiste en enviar de nuevo el mail, que, invariablemente, volverá a ser rechazado por la misma causa.**

▶ Usuario inexistente

En este caso, el nombre del servidor está bien escrito pero no existe el nombre de usuario (lo que está antes de la @) en ese servidor.

Si alguien enviara un mensaje a *nombre_de_usuario@yahoo.com* el mensaje de Yahoo, por ejemplo, diría (en caso de que esta dirección no exista):

```
"A mail message was not sent due to a
protocol error. 554 delivery error: dd
This user doesn't have a yahoo.com
account (nombre_de_usuario@yahoo.com) -
mta552.mail.yahoo.com"
```

en otros servidores podría ser así:

```
"The following recipients did not receive
the attached mail. Reasons are listed with
each recipient: <usuario@servidor.com>
Unknown Recipient"
```

▶ Casilla llena

Muchos servidores de mail gratuitos tienen un límite en el tamaño de las casillas. Si la casilla a la que estás enviando un mail está llena, éste no entrará.

El mensaje en este caso, para Yahoo por ejemplo, será:

```
"A mail message was not sent due to a
protocol error.
554 delivery error:
dd Sorry, your message to
nombre_de_usuario@yahoo.es cannot be
delivered.
This account is over quota. -
mta458.mail.yahoo.com"
```

▶ Tamaño del mail mayor al permitido por el servidor

Algunos servidores gratuitos tienen un límite para el tamaño de los mensajes entrantes.



► **Si el servidor nos está diciendo que la dirección que escribimos está mal, no sirve de nada insistir.**

Este puede ser de 1 Mb.

Si estamos enviando un mail con un tamaño mayor, éste no entrará.

El mensaje de rechazo dirá:

```
"A mail message was not sent due to a
protocol error.
1094833 bytes exceeds server limit of 1000000"
```

o también

```
"A mail message was not sent due to a
protocol error.
554 delivery error: dd Sorry your message to
nombre_de_usuario@yahoo.com.ar cannot be
delivered because it is too large. -
mta530.mail.yahoo.com"
```

► Cuenta desactivada

Puede suceder que la cuenta haya sido desactivada por distintos motivos.

En este caso, el mensaje dirá:

```
"A mail message was not sent due to a
protocol error.
554 delivery error: dd Sorry your message to
nombre_de_usuario@yahoo.com.ar cannot be
delivered.
This account has been disabled or
discontinued [#102]. - mta497.mail.yahoo.com"
```

Si el servidor nos está diciendo que la dirección que escribimos está mal, no sirve de nada insistir.

Muy probablemente no tengamos la dirección correcta o hayamos cometido algún error al escribirla.

Podremos insistir una vez más por si el servidor estuvo momentáneamente fuera de servicio o algún otro problema, pero no mucho más.

En algún caso muy esporádico este error puede deberse a otras causas pero en la inmensa mayoría de los casos, se trata de errores en la dirección.

Si querés mandar una carta por correo postal a la dirección Av. San Martín 3892 pero en el sobre escribís Av. San Martín 382 y la carta no llega a destino, no tiene sentido que le echés la culpa al Correo.



Cómo NO usar

el correo electrónico

Abusos cometidos con el mail

Hoaxes

Los hoaxes (broma, engaño) son mensajes de correo electrónico engañosos que se distribuyen en cadena.

Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que pueden sucederte si no reenvías el mensaje a todos los contactos de tu libreta de direcciones.

También hay hoaxes que tientan con la posibilidad de hacerte millonario con sólo reenviar el mensaje o que apelan a la sensibilidad invocando supuestos niños enfermos.

Hay otros que repiten el esquema de las viejas cadenas de la suerte que recibíamos por correo postal que te auguran calamidades si cortás la cadena y te prometen convertirte en millonario si la seguís.

He recibido muchas cadenas en las que se decía *"no sé si será cierto pero por las dudas yo lo reenvío"*.

Para los temerosos o supersticiosos, les cuento que yo he roto infinidad de cadenas y no me ha sucedido nada.

También he reenviado unas cuantas y no me he vuelto millonario.

Por eso te pido, no reenvíes estos mensajes, atrevete a romper las cadenas!



- ▶ **Los hoaxes (broma, engaño) son mensajes de correo electrónico que se distribuyen en cadena.**
- ▶ **No reenvíes estos mensajes. Atrevete a romper las cadenas!**

Categorías de hoaxes

Básicamente, podemos dividir los hoaxes en las siguientes categorías (en *Rompecadenas* podés encontrar los textos de más de 80 hoaxes):

- ▶ Falsas alertas de virus
- ▶ Mensajes de temática religiosa
- ▶ Cadenas de solidaridad
- ▶ Cadenas de la suerte
- ▶ Leyendas urbanas
- ▶ Métodos para hacerse millonario
- ▶ Regalos de grandes compañías

- ▶ Mensajes tomando el pelo a la gente que envía hoaxes
- ▶ Mensajes verdaderos pero que no deben ser reenviados

Hay otros mensajes que no nacen como hoaxes pero pueden tener sus mismas consecuencias:

- ▶ Poemas y mensajes de amor y esperanza (éstos suelen venir en un archivo de *Power Point* pesadísimo).
- ▶ Mensajes para unirte a programas de afiliados.
- ▶ Chistes y fotos que circulan en cadena.

Falsas alertas de virus

La mayoría de las alertas de virus que nos llegan por mail son falsas.

Todas empiezan diciendo que ayer se descubrió un nuevo virus (¿cuándo es ayer en *Internet*?) que no tiene cura. Lo dijo la *CNN* (vas a la página de la *CNN* y no hay nada sobre ese supuesto virus).

Después dicen que el virus borrarán todos los datos de tu disco rígido, algunos incluso dicen que además dejará de funcionar el *Internet Explorer*!

Finalmente te piden que reenvíes el mensaje a toda tu libreta de direcciones.

Pero algunas alertas son verdaderas. De todos modos, no sirve enviar ninguna alerta de virus, ni siquiera las verdaderas porque ¿cómo distinguir las de las falsas?

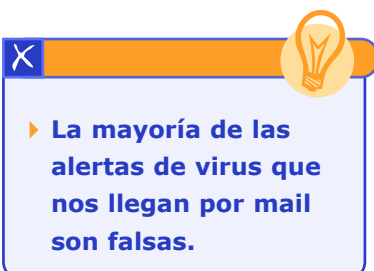
Lo mejor es suscribirse a algún boletín que envíe este tipo de información.

En el *Directorio Rompecadenas* podés encontrar algunos sitios que ofrecen este servicio.

Por otro lado, no hay ningún virus que no tenga cura. Generalmente los fabricantes de programas antivirus a las pocas horas o a los pocos días de la aparición de un nuevo virus ponen en Internet a disposición de sus usuarios la actualización correspondiente.

Mensajes de temática religiosa

Las personas inescrupulosas que se dedican a recolectar direcciones de mail convierten oraciones, rezos e historias religiosas en hoaxes, agregando al final del mensaje alguna frase del tipo "si no



reenvías esta carta a toda tu libreta de direcciones, nada de lo que pidas se cumplirá” o cosas por el estilo.

No tengo nada en contra de estas oraciones, creo que deben ser respetadas.

Pero también creo que deben ser respetados aquellos que no quieren recibirlas, y, por supuesto, la privacidad de sus direcciones.

Consideraremos hoaxes a aquellos mensajes que, con alguna de estas estratagemas, inciten a ser reenviados.

Si no, son solamente mensajes que a alguien le parecen agradables o edificantes y encuentra que son buenos para compartir con otros.

Por lo tanto, sugiero, si sos religioso y querés compartir estos mensajes con tus amigos procedé de la siguiente manera: (este procedimiento también es recomendable para aquellos que gustan de enviar chistes o bromas):

- ▶ preguntale a tus amigos si quieren recibir este tipo de mensajes y envíalos sólo a quienes te contesten afirmativamente.
- ▶ eliminá aquellas partes en las que se pide que el mensaje sea reenviado ya que, te lo aseguro, ningún deseo o pedido dejará de cumplirse porque no envíes un mail, ni se cumplirá porque lo envíes.



- ▶ **Las falsas cadenas de solidaridad son verdaderamente detestables.**
- ▶ **Juegan con la sensibilidad del receptor.**
- ▶ **Perjudican a todas las cadenas que pudieran ser creadas por gente que realmente lo necesita.**
- ▶ **Quienes pretenden ayudar, en realidad están perjudicando.**
- ▶ **Reenviando estos mails no ayudás a nadie.**

Cadenas de solidaridad

Las falsas cadenas de solidaridad son verdaderamente detestables.

Por un lado juegan con la sensibilidad del receptor (*"no perdés nada reenviando este mail y un pequeño niño puede salvar su vida"*).

Por otro lado, perjudican a todas las cadenas que pudieran ser creadas por gente que realmente lo necesita.

Por lo tanto se da la paradoja de que quienes pretenden ayudar reenviando estos mensajes, en realidad están perjudicando.

Reenviando estos mails no ayudás a nadie.

Por el contrario, contribuís a la confusión general.

Si querés ayudar a gente que realmente lo necesita podés visitar los sitios de algunas instituciones solidarias incluidos en el *Directorio Rompecadenas*.

Si vos sos el que necesita ayuda, podés conectarte con alguna insti-

tución como *Red Solidaria*, que se encarga de vincular a personas que necesitan ayuda con aquellos que pueden brindársela.

Cadenas de la suerte

Las cadenas de la suerte son el equivalente de las viejas cadenas que recibíamos por correo postal ("*envíe esta carta a cinco personas. José Pérez no las envió y a la semana murió aplastado por un camión. Nilda Gutiérrez las envió y a los dos días ganó la lotería*").

Por supuesto, son una gran mentira.

Yo he roto infinidad de cadenas y no me ha sucedido nada. Por otro lado, he reenviado algunas y no me he vuelto millonario.

Leyendas urbanas

Increíbles, fascinantes, absurdas, atrapantes.

Las leyendas urbanas, que antes se transmitían oralmente, ahora se propagan por el correo electrónico, ya que son perfectas para ser utilizadas como hoaxes.

Las leyendas urbanas son esas historias que circulan de boca en boca (y en los últimos años a través del correo electrónico) y que mucha gente da por descontado que son ciertas.

Por ejemplo, es famosa en todo el mundo la leyenda de que *Walt Disney* se hizo congelar hasta que se creara una cura para el cáncer. Esta, como la mayoría de las leyendas urbanas, es falsa.


No dejan de ser historias fascinantes, incluso algunas están magistralmente escritas, pero no deben ser creídas y mucho menos reenviadas por correo electrónico ya que persiguen la finalidad de cualquier hoax: recolectar direcciones de mail para ser utilizadas por los spammers.

Métodos para hacerse millonario

Estos hoaxes son el equivalente, por correo electrónico, de las clásicas pirámides para hacer dinero.

He probado un par de pirámides y, creeme, no funcionan.

Leyendo las instrucciones te parecerá lógico y hasta irrefutable que



▶ **Las leyendas urbanas no dejan de ser historias fascinantes, incluso algunas están magistralmente escritas, pero no deben ser creídas y mucho menos reenviadas por correo electrónico ya que persiguen la finalidad de cualquier hoax: recolectar direcciones de mail para ser utilizadas por los spammers.**



► **El reenvío de hoaxes cuesta la privacidad de todos los que utilizamos el correo electrónico.**



se puede ganar dinero con las pirámides.

Pero yo te digo algo más lógico: es imposible que todos ganen. Si alguien gana, muchos pierden. Y lo más probable es que vos estés entre los que pierdan.

Regalos de grandes compañías

Estos hoaxes son realmente graciosos.

El que más me gusta es el que dice que *Microsoft* y *AOL* pagarán u\$s 245 por cada mail que envíes.

¿Cómo pueden saber que yo estoy enviando un mail para poder pagarme?

Por otro lado, con que unos cuantos miles de personas manden algunos cientos de mails, se fundirían.

Pero la credulidad de alguna gente no tiene límites.

Recibí este hoax de una persona. No le dí importancia y lo borré. A los seis meses volví a recibirlo de la misma persona.

No podía creerlo. Le escribí preguntándole si la primera vez había recibido algún cheque. Me dijo que no. Volví a escribirle preguntándole para qué me lo enviaba nuevamente. "*Por las dudas*" me contestó "*Total, no cuesta nada*".

No se lo dije porque advertí que se trataba de un caso perdido, pero pensé que sí, que cuesta muchísimo, cuesta la privacidad de todos los que utilizamos el correo electrónico.

Mensajes tomándole el pelo a la gente que envía hoaxes

Alguna gente, cansada de recibir hoaxes, envía a cada persona que le manda estos mensajes un mail exagerando un poco los daños que podría producir un supuesto virus.

La finalidad de estos mensajes es intentar concientizar sobre las consecuencias de reenviar cadenas por medio de la ironía.

Lo curioso es que estos mensajes que pretenden combatir los hoaxes terminan siendo también hoaxes.

Son mensajes burlándose de la gente que reenvía hoaxes, son

hoaxes sobre los hoaxes, vendrían a ser meta-hoaxes, bah, no sé, digo, qué se yo.

¿Servirán para algo? Espero que sí porque están circulando bastante.

Mensajes reales que no deben ser reenviados

Hay algunos mensajes que son ciertos o están basados en algún hecho real pero que, por diversas causas, no deben ser reenviados.

En general, se trata de campañas comenzadas por alguien hace años y que piden que la gente las "firme". Pongo firma entre comillas porque un nombre puesto en un mail no es una firma.

Cualquiera puede poner mi nombre en un mail sin mi consentimiento, incluso puedo estar en desacuerdo con lo que "firmé".

Si la campaña ya terminó o la persona que la inició se vio desbordada y dio de baja su cuenta de mail, no tiene ningún sentido agregar tu nombre a la lista, aunque lo que diga el mensaje sea verdad.

También sucede esto con mensajes de ayuda a personas enfermas pero que ya, o bien se curaron o fallecieron.

En este caso no harás más que molestarlos a ellos o a sus familiares.



Objetivos de los hoaxes:

- ▶ Conseguir direcciones de mail.
- ▶ Congestionar los servidores.
- ▶ Alimentar el ego del autor.

Algunos detalles sobre los hoaxes

Características


- ▶ No tienen firma (aunque algunos tienen falsas firmas, por ejemplo, *José Pérez, Gerente General Microsoft Latinoamérica*).
- ▶ Algunos invocan los nombres de grandes compañías.
- ▶ Piden al receptor que lo envíe a todos sus contactos.
- ▶ Te amenazan con grandes desgracias si no lo reenvías.

Objetivos

- ▶ Conseguir direcciones de mail.
- ▶ Congestionar los servidores.
- ▶ Alimentar el ego del autor.

Consecuencias

- ▶ Hacen perder tiempo y dinero al receptor.
- ▶ Congestionan los servidores.
- ▶ Nos llenan de publicidad y basura.
- ▶ Hacen perder valor a cadenas creadas por gente que realmente lo necesita.



▶ Hacen perder tiempo y dinero al receptor.


▶ Congestionan los servidores.

▶ Nos llenan de publicidad y basura.

Cómo actuar frente a los hoaxes

- ▶ No reenviar nunca estos mensajes. De todos modos casi ninguno merece la pena de ser reenviado.
- ▶ Explicarle a tus amigos cuáles son las consecuencias de reenviar estas cadenas y pedirles que no lo hagan más (si insisten, mandarlos a *Rompecadenas*).
- ▶ Al reenviar un mensaje, utilizando la opción *Reenviar mensaje* o *Forward* del programa de correo, se incorporan al mensaje todas las direcciones incluidas en los campos *Para* y *CC*.

Para evitar esto, si deseás reenviar a varias personas un mensaje que recibiste, procedé de la siguiente manera:



▶ No reenviar nunca estos mensajes.

▶ Explicarle a tus amigos cuáles son las consecuencias de reenviarlos.

- ▶ Seleccioná la parte del mensaje que deseás reenviar, evitando las direcciones.
- ▶ Copiá y pegá en un mensaje nuevo. De esta manera evitás que circulen todas las direcciones de mail que venían en el mensaje.
- ▶ Utilizá el campo *CCO* o *BCC*. Todas las direcciones que incluyas en estos campos no serán vistas por las personas que reciben el mensaje.

Algunas pautas para reconocer un hoax

Hay varios indicios para descubrir si un mensaje que recibimos en cadena es falso:

- ▶ Si incita a ser reenviado es altamente probable que se trate de un hoax.
- ▶ Si habla de un virus informático que no tiene cura, es seguro que se trata de un hoax (no hay virus que no tenga cura).
- ▶ Si habla de que algún ISP donará dinero a algún niño enfermo por cada mail reenviado es más que probable que sea falso (ningún ISP puede rastrear cada mail que se envía).
- ▶ Si promete regalos fabulosos de grandes compañías (*Microsoft, AOL, etc.*) seguramente es falso. Si la compañía no es conocida, mucho peor. Puede tratarse de un fraude o una estafa.
- ▶ Tienen un tono catastrófico. Ponen frases como "*Alerta!!! Urgente!!! Virus sin cura!!! Destruirá toda su información y su disco rígido!!!*"
- ▶ La mayoría no están firmados aunque hay algunos que tienen falsas firmas.
- ▶ No remiten a ningún sitio web donde comprobar la información.
- ▶ Y finalmente, podemos dirigirnos a los sitios especializados en hoaxes como *Rompecadenas, VS Antivirus, Virus Attack!* o *Urban Legends and Folklore*.

Cómo responder a quienes nos envían hoaxes

Algunas personas me han comentado que al reenviar una cadena han recibido insultos y amenazas.

Ya sé que estás cansado de que te llenen el buzón con mensajes falsos, pirámides para ganar dinero fácil, cadenas para ayudar a niños enfermos que no existen, etc.

Yo también lo estoy, por eso construí *Rompecadenas*.

Pero creeme que responder con insultos a los conocidos que te envían hoaxes no es la mejor manera de actuar ya que:

- ▶ la persona que recibe los insultos puede molestarse con nosotros.
- ▶ quizás no logremos lo que queremos (que no mande más cadenas).
- ▶ estamos perdiendo una gran oportunidad de ejercer nuestras habilidades pedagógicas.

Tal vez con insultos logremos que esa persona no nos envíe más cadenas por temor a ser insultada.

Pero no habrá aprendido nada.

Pensará algo como "no voy a enviarle mensajes a este loco que me insulta por mandarle un mail para ayudar a un niño enfermo" y quizás siga enviándolas a otras personas que no lo insultan.

La forma de actuar que te voy a proponer la conocí en *The Urban Legend Combat Kit* y me ha dado excelentes resultados.

Tal vez logres que esa persona deje de enviar cadenas y se sume a nuestra causa (hacer entre todos una *Internet* mejor).

Consiste en lo siguiente:

Agradecer el envío del mensaje con respeto para no ofender, comunicar que el mensaje es falso, explicar lo que es un hoax e invitar a conocer Rompecadenas o algún otro sitio que trate este tema.

Supongamos que alguien nos envía el hoax *Solidaridad con Brian* que habla sobre un supuesto niño enfermo.

En este caso mi respuesta es algo así:

"Hola, gracias por enviarme el mensaje Solidaridad con Brian.

Afortunadamente, es falso. Se trata sólo de un hoax (broma, engaño) que circula en cadena por correo electrónico.

La finalidad de estos mensajes es congestionar los servidores y obtener direcciones de mail para venderlas a quienes luego nos envían publicidad no solicitada.

Podés obtener más información en Rompecadenas

<http://www.rompecadenas.com.ar>

Saludos cordiales"

Si recibís el mensaje que dice que *Microsoft* pagará \$245 por cada mail que envíes, podés cambiar "afortunadamente" por "desafortunadamente" :-)

De esta forma, te lo aseguro, la mayoría de las personas dejan de enviar hoaxes (por lo menos a mí).

Estoy convencido de que la mejor forma de romper las cadenas es la información y el conocimiento.

No hay muchas personas que, conociendo las consecuencias, sigan reenviando estos mensajes (aunque hay algunos casos incurables).

Adicionalmente, vos quedarás muy bien ya que:

- ▶ los tratarás con respeto.
- ▶ quedará claro que sabés de lo que estás hablando.
- ▶ les habrás enseñado algo que no sabían.



▶ **La mejor forma de romper las cadenas es la información y el conocimiento.**

¿Tanto escándalo por unos cuantos mensajes falsos? ¿Acaso un hoax puede llegar a ser peligroso o es solamente una broma?

Los hoaxes pueden llegar a ser peligrosos en varias formas.

Además de las características comunes a todos los hoaxes (congestión de servidores, recolección de direcciones de mail) hay algunos que pueden perjudicarnos de otras maneras.

Por ejemplo, los titulados *Sulfnbk* o *Jdbgmgr*, falsas alertas que hicieron que muchísima gente borrara archivos de Windows creyendo que se trataba de virus.

Muchos hoaxes funcionan en base al miedo que generan y también pueden provocarnos pánico, terror, asco, etc.

Sin ir más lejos, la cantidad de hoaxes creados en relación a los atentados en Estados Unidos, generó miedo adicional en mucha gente.

También hay otro titulado *Taiwan Babies*, realmente asqueroso, en el que se ven fotos de una persona comiendo lo que aparenta ser un feto humano. En realidad es un pato con una cabeza de muñeco. Pero mucha gente termina de ver las fotos asqueada y sensibilizada.

Por otro lado, debemos tener mucho cuidado con los mensajes que involucran a personas o empresas reales, ya que es muy fácil utilizar este medio para difamar o calumniar (un ejemplo de esto es el hoax que vinculaba al grupo musical *La oreja de Van Gogh* con *ETA* o el hoax llamado *La coima del siglo*, que difamaba al programa televisivo argentino *Telenoche Investiga*).

Finalmente, un fenómeno que estoy observando con mucha frecuencia últimamente, es que se toma algún hoax existente y se le insertan todos los datos de alguna persona real (nombre, cargo, lugar de trabajo, TE, mail), generalmente profesionales, para darle mayor seriedad al mensaje.

No hace falta decir las molestias que esta situación puede causarle a esta persona que aparece avalando supuestamente determinada información (cientos de mails, llamados telefónicos, abogados, cartas documento, etc.).



- ▶ **Los hoaxes pueden llegar a ser peligrosos en varias formas.**
- ▶ **Congestión de servidores.**
- ▶ **Recolección de direcciones de mail.**
- ▶ **Hay gente que borró archivos de su sistema operativo creyendo que se trataba de un virus, a causa de un hoax.**
- ▶ **Algunos funcionan en base al miedo que generan y también pueden provocarnos pánico, terror, asco, etc.**
- ▶ **También es muy fácil utilizar este medio para difamar o calumniar.**

Reenviar un mail también puede hacer daño

"No sé si será cierto, por las dudas lo reenvío".

Esta infeliz frase acompaña varias cadenas de mail.

La frase que debería pasar por la cabeza de quien recibe una cadena es *"no sé si será cierto, por las dudas NO lo reenvío"*.

Con un simple mail se puede hacer daño a mucha gente.

Además de saturar las casillas de correo que figuran en estas cadenas, es muy fácil difamar y ensuciar a personas, instituciones, programas de televisión, grupos musicales, etc.

Las cadenas de mail están siendo utilizadas como forma de difamar y ensuciar a competidores o simplemente a alguien a quien le tenemos bronca.

Es innumerable la cantidad de personas que se han visto perjudicadas por maniobras de este tipo y grande también el daño causado.

Seguramente recordarás un mail de una supuesta ex empleada del programa periodístico argentino *Telenoche Investiga* despedida y amenazada a raíz de una investigación realizada.

El mensaje, falso, además de difamar a *Telenoche Investiga*, llevaba el nombre y número de documento de una persona ajena totalmente al programa y que se vio altamente perjudicada por esta cadena.

Numerosos llamados telefónicos, la publicación de sus datos personales, DNI, número de su cuenta bancaria, llamadas de su banco, verse mezclada con abogados, cartas documento, etc., son algunos de los perjuicios a los que se vio sometida esta persona, por el sólo hecho de que a un estúpido se le ocurrió poner su nombre en una cadena de mails.

Esta maniobra es una de las más bajas que puedan verse: utilizar el nombre de una persona para difamar a otro.

Los hoaxes son creados por delincuentes y difundidos por gente honesta.

Una vez más los inescrupulosos se valen de los sentimientos de las personas para hacer daño o recolectar direcciones de mail.

No es verdad que *"reenviar un mail no cuesta nada"* como dicen algunos hoaxes.

Cuesta y mucho:

- ▶ las direcciones de mail y la privacidad de todos los usuarios de Internet.
- ▶ la privacidad y el nombre de quienes son víctimas de estas maniobras.



▶ ***"No sé si será cierto, por las dudas lo reenvío".***

Esta infeliz frase acompaña varias cadenas de mails.

▶ **La frase que debería pasar por la cabeza de quien recibe una cadena es *"no sé si será cierto, por las dudas NO lo reenvío"*.**

▶ **Las cadenas de mail están siendo utilizadas como forma de difamar y ensuciar.**

▶ **Los hoaxes son creados por delincuentes y difundidos por gente honesta.**

▶ **No es verdad que *"reenviar un mail no cuesta nada"*. Cuesta, y mucho.**



- ▶ **Todos podemos llegar a ser víctimas de estos delincuentes.**
- ▶ **Pensalo varias veces antes de reenviar una cadena que involucra a personas con nombre y apellido.**
- ▶ **Con tu click en *Reenviar* estarás siendo cómplice involuntario de la difamación.**

Todos podemos llegar a ser víctimas de estos delincuentes.

Imaginate que el día de mañana puede tocarte a vos y no te gustará ver tu nombre difamado en cientos o miles de mails.

Por eso, pensalo varias veces antes de reenviar una cadena que involucra a personas con nombre y apellido.

Con tu click en *Reenviar* estarás siendo cómplice involuntario de la difamación.

NO hoax
virus
spam

Rompecadenas
<http://www.rompecadenas.com.ar>

Spam



- ▶ **Se llama *Spam* a la práctica de enviar indiscriminadamente mensajes de correo no solicitados.**
- ▶ **Un tercio de los mails que se envían son spam.**
- ▶ **Es intolerable recibir una vez por semana el mismo mensaje sobre la necesidad de filtrar el agua de la ducha.**
- ▶ **La ley que invocan los spammers al final de sus mensajes no existe.**

Se llama spam a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas web.

Todos aquellos que tenemos una dirección de correo electrónico recibimos a diario varios mensajes publicitarios que no solicitamos sobre cosas que no nos interesan.

Habitualmente, después de haber recibido un hoax, comenzamos a recibir publicidad no solicitada.

Nuestra dirección ya ha sido incorporada a las bases de datos de los spammers, luego de haberla obtenido por medios, no ya ilegales porque no hay legislación sobre el tema en la mayoría de los países, pero sí inmorales.

A comienzos del año 2000 se calculaba que el 30% de los mails (varios cientos de millones por día) que se enviaban eran no solicitados, o sea, spam. Seguramente hoy son muchos más.

Por lo general, las direcciones son recolectadas por Internet o mensajes de correo o compradas.

Yo mismo recibo cada día dos o tres ofertas de bases de datos con millones de direcciones de email al increíble precio de u\$s 35.

Es intolerable recibir una vez por semana el mismo mensaje sobre la necesidad de filtrar el agua de la ducha.

Tampoco es agradable recibir un mensaje en formato HTML promocionando un nuevo servicio de distribución de videos, exclusivo para la ciudad de Buenos Aires, cuando yo vivo a miles de km. de distancia.

Esto, además de ofrecer una imagen negativa sobre la empresa que envía el spam, muestra la poca utilidad de las bases de datos compradas.

Por otro lado los spammers invocan una supuesta ley por la cual el mensaje que están enviando no puede ser considerado spam si tiene una forma de ser removido.

Esto es una gran mentira. Esa ley no existe.

Otros ponen "Su dirección fue tomada de un sitio público", pretendiendo justificar el spam.

En realidad lo que quieren decir es: "no vaya a creer que compré una base de datos de direcciones de mail, solamente encontré su dirección de correo en su página web, junté unas cuantas de esta manera y les he enviado un correo para ver si están interesados en mis servicios".

Además, la mayoría de las veces si uno contesta el mail pidiendo ser removido de la lista, lo único que hace es confirmar que su dirección existe.

Por lo tanto, es conveniente no responder nunca a un mensaje no solicitado.

Lo mejor es aplicar filtros o reglas de mensaje para evitar recibir mensajes de esas direcciones.

Otra opción muy buena, es quejarse al postmaster del que envía el spam, enviando un mail a `postmaster@dominio_del_spammer` o `abuse@dominio_del_spammer`.

Algo queda claro: el spam es perjudicial para todos, hasta para la empresa que lo envía.

Por otro lado, el spam es la publicidad más barata para el anunciante y la más cara para los receptores.


Cada vez que recibís un mensaje no solicitado, le estás pagando al spammer su publicidad.

¿Qué sentirías si varias empresas te llaman todos los días por cobrar para intentar venderte cosas que no te interesan sin posibilidad de rechazar las llamadas ni cortar la comunicación hasta que terminen de pasarte el mensaje?

Esto mismo sucede con el spam. Cada año, los usuarios gastan miles de millones de dólares en tiempo de conexión para descargar mensajes no solicitados.

Algunas personas le dan su dirección solamente a sus amigos y piensan, de esta manera, estar a salvo del spam.

Error! Los amigos son lo peor! Basta con que uno reenvíe una cadena sin ocultar las direcciones para que tu mail pueda ser incorporado en cualquier momento a las bases de datos de los spammers.



▶ La mayoría de las veces si uno contesta el spam pidiendo ser removido de la lista, lo único que hace es confirmar que su dirección existe. Lo que logramos es recibir cada vez más spam.

▶ Es conveniente no responder nunca a un mensaje no solicitado.

▶ El spam es perjudicial para todos, hasta para la empresa que lo envía.

Por otro lado, uno no está aislado, Internet es una red, y si tu servidor se ve saturado por millones de mensajes de otros spammers esto también te afectará.

Si estás por hacer spam, te pido que lo pienses muy bien.
Si cada negocio o página web nos va a enviar aunque sólo sea un mail, el correo electrónico sería una herramienta absolutamente inservible.

Todos somos responsables de cuidar esta herramienta fabulosa.
Olvidate del spam como forma de promocionar tu negocio, hagamos entre todos una mejor Internet.



X

► **Si cada negocio o página web nos va a enviar aunque sólo sea un mail, el correo electrónico sería una herramienta absolutamente inservible. (Hoy ya hay miles de millones de páginas web en todo el mundo).**

Por qué NO conviene hacer spam

Porque el spam es perjudicial para todos.

El usuario que lo recibe:

- ▶ Pierde tiempo y dinero al descargar mensajes que no solicitó.
- ▶ Es molestado permanentemente con publicidad de cosas que no le interesan.
- ▶ Puede llegar un momento en que reciba más spam que mensajes que realmente le interesan.

El servidor al que pertenece la empresa o persona que lo envía:

- ▶ *Saturación del servidor:* imaginá cómo afecta a un servidor el envío de 1 millón de mails en tandas de 8.000 o 10.000.
- ▶ *Ingreso del servidor a listas negras:* Si el servidor recibe una denuncia es posible que ingrese en alguna de las listas negras que existen en Internet.

De este modo, los webmasters que consulten esas listas bloquearán el acceso de todos los mails provenientes de ese servidor (no sólo de la dirección que envía el spam ya que si no los spammers cambiarían continuamente su dirección y resolverían el problema).



El spam es perjudicial para todos:

- ▶ **El usuario que lo recibe.**
- ▶ **El servidor al que pertenece la empresa o persona que lo envía.**
- ▶ **La empresa o persona que lo envía.**
- ▶ **Todos los usuarios de Internet.**

La empresa o persona que lo envía:

- ▶ Podrá promocionar su negocio y tal vez vender un poco pero la mayoría de los receptores del spam sólo tendrán una imagen negativa.
- ▶ Su servidor podrá dar de baja su cuenta de correo electrónico para evitar que el spam afecte su rendimiento y para no figurar en listas negras.



▶ **Los usuarios gastan casi 10.000 millones de dólares al año para descargar publicidad que no solicitaron de cosas que no les interesan (año 2000).**

Todos los usuarios de Internet:

▶ Según una nota publicada en Terra "500 millones de avisos personalizados bombardean cada día las casillas de email de todo el mundo, según un estudio de la Comisión Europea.

Esto significa un costo de unos 9.360 millones de dólares al año para los usuarios, en función del tiempo de conexión utilizado" (datos válidos para el año 2000, hoy son muchísimos más).

Esto nos da una idea de cómo esta práctica afecta el rendimiento de toda la red.

Cómo se unen los hoaxes y el spam

El spam y los hoaxes están íntimamente ligados. Todo hoax tiene como finalidad el spam.

El principal objetivo de los hoaxes es conseguir direcciones de mail para luego armar bases de datos con el fin de enviar correo no solicitado.

Y aquí es donde se unen los hoaxes y el spam y vemos cómo dependen el uno del otro para existir.

Mientras que los spammers son los que lanzan muchos de estos mensajes, los hoaxes les proveen de direcciones para su actividad.

Cuando una persona recibe un hoax y lo reenvía a todos sus conocidos sin ocultar sus direcciones está ayudando a los spammers a armar sus bases de datos.

No es extraño que luego de recibir un hoax, de parte de un conocido que no ocultó las direcciones, comenzamos a recibir spam.

Además de la intrusión y la molestia que esto significa, debemos añadirle el tiempo perdido en seleccionar los mensajes que nos interesan de entre tanta basura.

Como si esto fuera poco, el spam es la única forma de publicidad en la cual el costo es casi nulo para el anunciante y bastante alto para los receptores.



- ▶ **El spam y los hoaxes están íntimamente ligados.**
- ▶ **Todo hoax tiene como finalidad el spam.**
- ▶ **No es extraño que luego de recibir un hoax, de parte de un conocido que no ocultó las direcciones, comenzamos a recibir spam.**
- ▶ **El spam es la única forma de publicidad en la cual el costo es casi nulo para el anunciante y bastante alto para los receptores.**

Esto es totalmente inaceptable.

Todos los usuarios de Internet gastan miles de millones de dólares al año para descargar mensajes que no les interesan en concepto de gastos de conexión.

Este es uno de los puntos más cuestionados del spam y el que más bronca causa entre los usuarios.

Como ya vimos, el spam es perjudicial para todos, incluso para la empresa o persona que lo envía ya que llegar a través de un mensaje no solicitado, y obligar al receptor a pagar por él, no es la mejor manera de empezar una relación comercial con un cliente.

La mayoría (por no decir todos) de los expertos en marketing y promoción online desaconsejan severamente la práctica del spam como forma de hacer negocios en Internet.

Ciertamente, es mucho más productivo tener una base de datos de 1.000 personas que quieren recibir nuestras ofertas, que enviar un millón de mails a personas a las que no les interesan y que se formarán una mala imagen de nuestra empresa.

Además, nuestro proveedor de acceso a Internet podrá bloquearnos nuestra cuenta debido a las quejas recibidas.

Por otro lado, los spammers apelan a diversas artimañas, muchas de ellas cuando menos poco éticas, como utilizar direcciones gratuitas o inexistentes, falsificar sus direcciones, o utilizar servidores ajenos mal configurados para enviar sus mensajes.

Cuando envían cientos de miles de mensajes y ponen como dirección de respuesta una dirección existente o no de un servidor gratuito como Yahoo o Hotmail, están desviando a sabiendas a ese servidor unos cuantos miles de mensajes por rebotes, insultos, etc.

Y esto lo hacen muchísimos spammers cada día utilizando los servidores de estos sitios y obligando a los administradores a tener muchísimo trabajo extra borrando cientos y cientos de cuentas y mensajes.

Cuando utilizan servidores ajenos mal configurados (que permiten el relay), están usando los recursos de otro, lo cual constituye un robo.



- ▶ **Obligar al receptor a pagar por un mensaje no solicitado no es la mejor manera de empezar una relación comercial con un cliente.**
- ▶ **Ningún experto en marketing y promoción online aconseja la práctica del spam como forma de hacer negocios en Internet.**
- ▶ **Es mucho más productivo tener una base de datos de 1.000 personas que quieren recibir nuestras ofertas, que enviar un millón de mails a personas a las que no les interesan.**

Cómo actuar frente al spam

- ▶ No responder nunca un mensaje no solicitado. Lo único que harás es confirmar que tu dirección está activa.
- ▶ No te recomiendo bajo ningún punto de vista que respondas uno de estos mensajes con insultos y cosas por el estilo. Puede volverse en tu contra (nunca se sabe quién está del otro lado).
- ▶ Quejarte al postmaster de la persona que realiza el spam, enviándole una copia del mensaje recibido con los encabezados incluidos.
- ▶ Configurar filtros o reglas de mensaje en nuestro programa de correo para no recibir más mensajes de una dirección determinada.
- ▶ No dejar tu dirección de mail en cualquier formulario o foro de Internet.
- ▶ No dejar tu dirección de mail en cualquier cupón, formulario, sorteo, etc., fuera de Internet.
- ▶ Muchos sitios tienen una *Política de privacidad*. En general, esto significa que se comprometen a no ceder los datos de sus usuarios, suscriptores, etc.
Si vas a dejar tu dirección de mail en algún formulario o foro, busca en el sitio esta *Política de privacidad*.
- ▶ Si estás recibiendo demasiado correo basura, tal vez lo mejor sea cambiar tu dirección de correo.

La situación en la Argentina

La *Secretaría de Comunicaciones* de la Argentina ha presentado a las Cámaras de Diputados y Senadores, a fines del 2001, un Anteproyecto de ley titulado *Regulación de las comunicaciones comerciales publicitarias por correo electrónico*.

De aprobarse, esta ley será una herramienta fundamental para la lucha contra el spam ya que brindará a los receptores la posibilidad de dejar de recibir correo publicitario no deseado y de reclamar indemnizaciones para quienes sigan enviando estos mails contra el deseo del destinatario.

También facultará a proveedores de acceso y de correo electrónico a demandar, solicitar indemnización y cancelar las cuentas de quienes no respeten esta norma, así como para filtrar el spam que reciben.

Lamentablemente, hay quienes creen que el spam no es un problema grave y que quienes nos quejamos somos personas quisquillosas a las que nos molesta recibir uno o dos mensajes no solicitados por semana.

De hecho, este es un problema gravísimo: quienes usamos el correo electrónico desde hace años recibimos en nuestras cuentas decenas de estos mensajes por día y debemos pagar para descargarlos y perder tiempo para enviarlos a la basura, que es donde siempre van a parar.

Además de perjudicar a los usuarios esta práctica le ocasiona muchos gastos y problemas a los ISPs (proveedores de acceso a Internet) y lo más grave de esta situación es que en este momento, y debido a la gran cantidad de spam proveniente de Argentina, algunos proveedores de otros países están comenzando a filtrar varios dominios o proveedores de la Argentina, e incluso el .ar entero.

Esto significa que tus mails no le llegarán a los usuarios de esos proveedores.

Y se lo debemos a un puñado de spammers apañados por sus proveedores que no hacen nada para evitarlo.


Esta gente nos está llevando a un cyberghetto y lamentablemente el anteproyecto de ley está totalmente parado debido a la grave situación que vive el país.



- ▶ **Lamentablemente, hay quienes creen que el spam no es un problema grave y que quienes nos quejamos somos personas quisquillosas a las que nos molesta recibir uno o dos mensajes no solicitados por semana.**
- ▶ **Hay quienes reciben decenas o cientos de spams por día.**
- ▶ **Algunos proveedores de otros países están comenzando a filtrar varios dominios o proveedores de la Argentina, e incluso el .ar entero.**
- ▶ **Se lo debemos a un puñado de spammers apañados por sus proveedores.**
- ▶ **Esta gente nos está llevando a un cyberghetto.**



Virus

X 

- ▶ **No alcanza con tener un antivirus instalado: si no se lo actualiza periódicamente es prácticamente lo mismo que no tenerlo.**
- ▶ **Hacer un backup periódico de los datos.**
- ▶ **Lo importante no es la computadora sino lo que está adentro.**
- ▶ **Una computadora vale unos cuantos cientos de dólares, pero ¿cuánto vale tu trabajo?**
- ▶ **El comportamiento del usuario es fundamental.**

Debido a la difusión que está teniendo Internet y a que enviar y recibir mails son acciones bastante sencillas de realizar, cualquier persona sin conocimientos de informática compra una PC, contrata una cuenta de correo electrónico y comienza a enviar mails.

Pero al poco tiempo se da cuenta de que necesariamente debe aprender muchas otras cosas si quiere mantener una correspondencia electrónica satisfactoria.

Uno de los principales problemas con los que se encuentra son los virus informáticos.

No alcanza con tener un antivirus instalado: si no se lo actualiza periódicamente, es prácticamente lo mismo que no tenerlo.

En rigor, debería ser actualizado en forma diaria para que cumpliera realmente la tarea para la que fue diseñado.

Pero muchísima gente no actualiza sus antivirus con esta frecuencia, ni siquiera en meses o años!

He visto computadoras con antivirus instalados 3 años atrás y que jamás habían sido actualizados.

Esto, prácticamente, puede ser el certificado de defunción de la información guardada en esa computadora.

Por otro lado, si el antivirus no fue actualizado en años, es probable que tampoco se hayan realizado copias de resguardo de la información.

Tuve mi primera experiencia con los virus informáticos hace más de 10 años, a comienzos de los 90, cuando el *Stoned* hizo humo mi trabajo de meses.

Por supuesto, tampoco había hecho un backup.

En ese momento, aprendí y decidí algunas cosas:

- ▶ Jamás volvería a pasarme algo similar.
- ▶ De allí en adelante haría un backup periódico de mi información.
- ▶ Lo importante no es la computadora sino lo que está adentro. Si me roban la computadora, o ésta se daña, de alguna manera, aunque me cueste, podré comprar otra.

Pero mi trabajo de meses o años es imposible de recuperar.

Una computadora vale unos cuantos cientos de dólares, pero ¿cuánto vale tu trabajo?

Por eso, el comportamiento del usuario es fundamental.

La gran mayoría de los daños producidos por virus se deben al comportamiento del propio usuario.

Con un poco de sentido común y unos sencillos consejos estarás muy bien protegido contra los virus.

Tu comportamiento determinará si te infectás o no.

No hay por qué tenerle miedo a los virus. Sólo hay que tener cuidado y estar informado.

Por supuesto también es imprescindible tener instalado un buen antivirus.

Pero si no te ocupás de actualizarlo no te servirá de nada.

Y lo más importante es tu comportamiento frente a los archivos que dejás entrar en tu computadora: a través del correo electrónico, de un chat, del ICQ, desde un diskette, o descargado desde internet, hay que ser muy precavido a la hora de abrir cualquier archivo.

Algunas recomendaciones:

- ▶ Nunca abras archivos no solicitados.
Sé que algunas veces la curiosidad puede más, pero ni la mejor foto ni el mejor chiste ni la mejor tarjeta de Navidad justifica que dejes entrar un virus en tu computadora.
- ▶ Instalá un buen antivirus y actualizalo permanentemente.
- ▶ Informate sobre nuevos virus en sitios especializados.
- ▶ Si tenés dudas sobre un archivo que recibiste de un conocido, antes de abrirlo escribible preguntándole si realmente te lo envió él y de qué se trata.
También podés guardar el archivo sin abrirlo en cualquier directorio de tu disco rígido y chequearlo con un antivirus actualizado.
- ▶ Cada vez que envíes un archivo poné una leyenda tipo «te envío adjunto un archivo sobre tal tema» y agregá tu nombre para que el destinatario sepa que no se trata de un virus enviado en forma automática desde una computadora infectada.
- ▶ Asegurate de que tu archivo salga sin virus.
- ▶ Hacé un backup de todos tus datos importantes.



- ▶ **La gran mayoría de los daños producidos por virus se deben al comportamiento del propio usuario.**
- ▶ **Nunca abras archivos no solicitados.**
- ▶ **Instalá un buen antivirus y actualizalo permanentemente.**
- ▶ **Informate sobre nuevos virus en sitios especializados.**
- ▶ **No reenvíes alertas de virus inexistentes.**



- ▶ **Deshabilitá la vista previa en Outlook Express.**
- ▶ **Deshabilitá el envío de mensajes en formato HTML.**
- ▶ **Instalá los parches correspondientes a tu navegador.**

- ▶ No reenvíes alertas de virus inexistentes para no confundirlos con los verdaderos.
- ▶ Nunca abras un archivo que te haya enviado un desconocido en un chat o por algún programa de mensajería.
- ▶ Deshabilitá la *Vista previa* en *Outlook Express* para evitar infecciones inmediatas de virus que infectan con sólo ver el mensaje, como *Badtrans* o *Klez*.
Para hacerlo, andá a *Ver > Diseño o Distribución* (según la versión de OE) y desactivá *Usar Panel de vista previa*.
- ▶ Deshabilitá el envío de mensajes en formato HTML.
Andá a *Herramientas > Opciones > Enviar > Formato para el envío de correo* y allí seleccioná *Texto sin formato*.
También es conveniente desactivar la opción *Responder a mensajes en el formato en que fueron enviados*.
- ▶ Instalá los parches correspondientes a tu navegador.
Los parches son correcciones que los fabricantes de software distribuyen para reparar errores o vulnerabilidades descubiertas en sus programas.
En este caso, es fundamental que instales los parches correspondientes a tu navegador para evitar la acción de programas que se aprovechan de esas vulnerabilidades.

>>> ¡¡¡¡ CUIDADO !!!!! ¡¡¡¡ NUEVO VIRUS !!!!!
 >>> NO HAY CURA... DESTRUIRA TU DISCO RIGIDO
 >>> ADEMÁS INUTILIZARA EL INTERNET EXPLORER
 >>> ¡¡¡¡ URGENTE !!!!! AVISEN A LOS QUE PUEDAN...

No hay ningún virus sin cura.

ATREVETE A ROM
 PER LAS CADENAS
<http://www.rompecadenas.com.ar>



Información complementaria

Enlaces

Rompecadenas

<http://www.rompecadenas.com.ar>

Directorio Rompecadenas

<http://www.rompecadenas.com.ar/directorio>

Freeware recomendado

<http://www.rompecadenas.com.ar/freeware.htm>

▶ **Hoaxes**

Rompecadenas

<http://www.rompecadenas.com.ar/hoaxes.htm>

Virus Attack!

<http://virusattack.virusattack.com.ar/hoaxes/>

VS Antivirus

<http://www.vsantivirus.com/hoaxes.htm>

Hoaxbusters

<http://hoaxbusters.ciac.org/>

Vmyths

<http://vmyths.com/index.cfm>

▶ **Virus**

VS Antivirus

<http://www.vsantivirus.com>

Virus Attack!

<http://www.virusattack.com.ar>

▶ Spam

Spambusters

<http://www.spambusters.org.ar>

Euro Cauce

<http://www.euro.cauce.org/es/index.html>

Anti Spam Argentina

<http://www.antispam-argentina.8m.net/>

Sobre el abuso en el servicio de correo electrónico

<http://www.rediris.es/mail/abuso/>

▶ Leyendas urbanas

Urban Legends and Folklore

<http://urbanlegends.about.com/science/urbanlegends/>

Urban Legends Reference Pages

<http://www.snopes2.com/>

The Urban Legends Combat Kit

<http://netsquirrel.com/combatkit/>

Diccionario de mitos y leyendas

<http://www.cuco.com.ar>

Leyendas urbanas.com

<http://www.leyendasurbanas.com/>

La página de los asustadores, el hombre de la bolsa y mil espantos tremebundos

<http://encina.pntic.mec.es/~agonza59/index.html>

▶ **Instituciones solidarias**

Red Solidaria

<http://www.redsolidaria.org.ar>

Chicos Perdidos

<http://www.chicosperdidos.org.ar>

▶ **Parches**

Virus Attack!

<http://virusattack.virusattack.com.ar/parches/>

▶ **Otros**

Netiquette

<http://www.geocities.com/Colosseum/Track/9699/netiquet1.html>

Outlook Express Backup

http://www.softonic.com/informacion_extendida.phtml?n_id=14706&plat=1

Distribución de este e-book

Está autorizada la distribución gratuita de este libro, por parte de cualquier persona y por cualquier medio, aunque sin alterar su contenido.

Deberán consignarse además los siguientes datos:

Guía de uso del correo electrónico

Eugenio Siccardi

Rompecadenas

<http://www.rompecadenas.com.ar>

Si este libro o alguno de sus capítulos fuera reproducido se agradecerá comunicarlo por mail a:

info@rompecadenas.com.ar

Acerca del autor

Eugenio Siccardi

Escritor, diseñador web.

Nació en Buenos Aires, Argentina en 1967.

Actualmente trabaja en un ISP (proveedor de acceso a Internet), por lo que constantemente es testigo de las malas prácticas en las que incurre la gente al utilizar el correo electrónico (por desconocimiento o mala intención).

Curtido receptor de los más diversos hoaxes, spam y virus desde hace varios años, se inició en esta actividad al advertir la falsedad de *Solidaridad con Brian*, hoax que, debe confesarlo, también reenvió.

Convencido de la enorme importancia del correo electrónico, dedica todos sus esfuerzos a ayudar a concientizar sobre el buen uso del e-mail.

Publicó también:

- ▶ **Cómo escribir un mail.** E-book, 37 p. Año 2002.
<http://www.rompecadenas.com.ar/escribirmail.htm>
- ▶ **Imágenes de la memoria.** *La creación de un banco digital de imágenes de El Bolsón.* Junto a Sergio Caviglia. Año 2002.
<http://www.rompecadenas.com.ar/memoria.htm>
- ▶ **Cuerpos obligatorios.** Poesía. Ediciones Topatumba. 60 p. Año 1992.
- ▶ Dirigió la revista de poesía "**Topatumba**".
- ▶ Tradujo, junto a Gianni Siccardi, una antología de poemas de **Salvatore Quasimodo**, para la colección Los Grandes Poetas (Centro Editor de América Latina) Año 1989.
- ▶ **Poemas y cuentos suyos** fueron publicados en diversas antologías y revistas de Argentina y Colombia.

Vive en El Bolsón, Patagonia, Argentina.

info@rompecadenas.com.ar

Acerca de Rompecadenas

Creado por *Eugenio Siccardi* en diciembre del año 2000, *Rompecadenas* es un sitio web destinado a orientar sobre el buen uso del correo electrónico.

Fundamentalmente, busca concientizar y ayudar a detener el envío de hoaxes, spam, virus y otras basuras que nos llegan por e-mail.

Al momento de realizar este e-book ofrece los siguientes recursos en forma gratuita:

- ▶ Artículos, Trucos y Consejos sobre hoaxes, spam y virus
- ▶ Directorio de enlaces relacionados
- ▶ Investigación y análisis de hoaxes
- ▶ Archivo con más de 80 hoaxes
- ▶ E-books gratuitos
- ▶ Leyendas urbanas
- ▶ Netiquette
- ▶ Freeware recomendado
- ▶ Boletín de novedades

Cuenta con una amplia red de colaboradores voluntarios de varios países de América y de España que constantemente envían los hoaxes que reciben para su inclusión en *Rompecadenas*.

<http://www.rompecadenas.com.ar>

Para suscribirte gratuitamente al boletín enviá un mail en blanco a rompecadenas-alta@eListas.net o completá el formulario en las páginas de *Rompecadenas*.

Colaborar con Rompecadenas

Numerosas personas me ayudan a romper cadenas de las siguientes formas:

▶ Enviando un hoax

Si recibiste algún hoax que no aparece en *Rompecadenas*, envíalo a info@rompecadenas.com.ar

▶ Enlaces y banners

Insertá un enlace o un banner de *Rompecadenas* en tu sitio.

Los enlaces pueden ser de la siguiente manera:

Rompecadenas

Todo sobre los hoaxes, spam, virus y otras basuras que nos llegan por e-mail.

<http://www.rompecadenas.com.ar>

Podés descargar los banners de

<http://www.rompecadenas.com.ar/enlaza.htm>

- ▶ Descargá la imagen que elijas (*botón derecho sobre la imagen, Guardar imagen como*).
- ▶ Insertá la imagen en tu sitio.
- ▶ Enlazá la imagen a <http://www.rompecadenas.com.ar>

▶ Reproduciendo artículos

Copíá cualquier artículo de esta guía o de *Rompecadenas* sin pedir permiso.

A cambio te pido que coloques un banner o un enlace a *Rompecadenas*.

Si querés recibir mis artículos por mail para reproducirlos en tu sitio web o publicación impresa, enviame tus datos (nombre, dirección de mail, url, nombre de la publicación) a info@rompecadenas.com.ar.

Recibirás uno o dos artículos mensuales simultáneamente con su publicación en *Rompecadenas*.

▶ Distribuyendo esta guía

Distribuí en forma gratuita esta guía entre tus amigos y conocidos. Pero cuidado! Controlate! No se te ocurra hacer spam!

Webmaster

Distribuí gratuitamente esta guía entre tus visitantes.

A cambio te pido que coloques un banner o un enlace a *Rompecadenas*.

▶ Suscribiéndote al boletín

Suscribite al boletín de *Rompecadenas* y recibí periódicamente las novedades producidas en el sitio, información sobre nuevos hoaxes, artículos, etc.

Para suscribirte gratuitamente enviá un mail en blanco a rompecadenas-alta@eListas.net

o completá el formulario en las páginas de *Rompecadenas*.

Agradecimientos

Quiero agradecer y dedicar este libro a las siguientes personas:

A Claudia Burman

por su constante aporte a *Rompecadenas* y por ayudarme a analizar y reflexionar sobre todos los aspectos del correo electrónico.

A José Luis López, de VS Antivirus

por todo lo que he aprendido de él sobre hoaxes y virus y por los conocimientos que comparte diaria y desinteresadamente con tanta gente.

Y a todos los integrantes de la lista *VS Ayuda*.

A Maximiliano Kulus, de Spambusters

por todo lo que he aprendido de él sobre el spam y por su permanente lucha antispammer.

Y a todos los integrantes de la lista *Spambusters*.

A todos los que colaboran con Rompecadenas

enviando comentarios, sugerencias, hoaxes o escribiendo artículos.

A todos los usuarios de elbolson.com

quienes con sus consultas me han ayudado a organizar y sistematizar esta información.

A mi padre, Gianni Siccardi

por haberme enseñado a escribir.

A mi hermana, Yanina Siccardi

A mi esposa, Mónica Sicouly

A mis hijos, Dante y Mateo